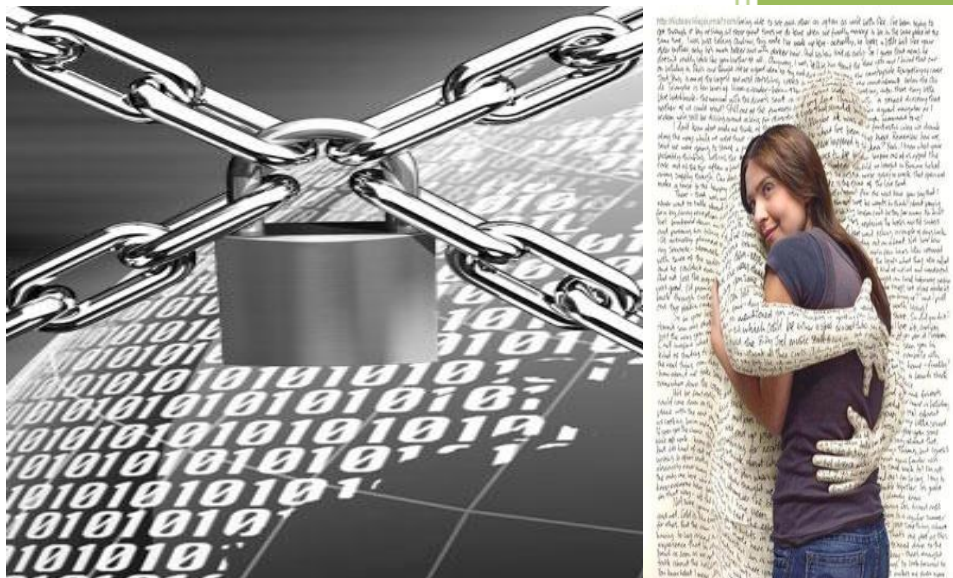
Faculdade de Letras da Universidade do Porto
Preservação e Conservação

Jan. 2011

Segurança da Informação

Trabalho Realizado por:
Sofia Elisabete Costa
Patrícia Lopes

Agradecimentos

Antes de avançar com este trabalho, queremos manifestar o nosso agradecimento à Prof. Doutora Manuela Pinto, sem a qual não seria possível dar continuidade ao trabalho que a seguir se apresenta e consequentemente, levá-lo a bom termo.

Sumário

Índice de Ilustrações

Resumo

Na emergente era da informação, a segurança da informação é uma preocupação cada vez mais presente no dia-a-dia das organizações. Desengane-se quem pensa que apesar da constante evolução tecnológica as ameaças à segurança da informação estão apenas relacionadas com as novas tecnologias. Não deixa de ser verdade, que com as novas tecnologias se tem vindo a desenvolver um vasto leque de armas que muito contribuem para o aumento da insegurança da informação – como exemplo temos: programas de *spyware*, *adware*, vírus informáticos, etc. – no entanto, não se pode colocar de parte uma enorme ameaça que nada tendo a ver com os meios tecnológicos, é apelidada de *Engenharia Social*.

De forma paralela ao aparecimento destas ameaças, foram também sendo desenvolvidas respostas, tanto no âmbito tecnológico como no âmbito da engenharia social. Para combater as ameaças de origem tecnológica foram sendo desenvolvidos programas de *anti-spyware*, *anti-adware*, *anti-virus*, etc. Quanto á engenharia social, pouco mais se pode fazer do que preparar os colaboradores das instituições para enfrentar determinadas técnicas utilizadas pelos engenheiros sociais. Atenção! Não existem medidas 100% eficazes contra a violação da informação.

Existem ainda duas Normas Internacionais pertencentes à família ISO, que devem ser empregues pelas instituições, não para resolver problemas de violação da informação, mas para evitar que esses problemas aconteçam. Trata-se das Normas ISO 17799 e 27001. Paralelamente a tudo isto e para combater os crimes relacionados com a segurança da informação, vão sendo postos em prática vários instrumentos legais.

Abstract

In the information age, the organizations are each time more concerned whit the information security. And although new technologies are in constantly evolution, there are more treats to the information security. It’s true that with the new technologies appeared many weapons that can be used to break the information security systems – some examples are: spyware and adware programs, computer viruses, etc. – but, it’s also true that there is another treat, perhaps even older than those mentioned treats, we are talking about the *Social Engeneering*.

To fight against these treats were being developed technologic and social answers. To defeat the technologic treats, the experts are developing anti-spyware and anti-adware programs, antivirus, etc.. To defeat the Social Engineer, we can’t do much more than prepare the

institution's employees though training programs. But, it's very important remember that there are no 100% effective measures against problems related with the information security.

There are two ISO International Standards that the institutions should respect. Those Standards help their to avoid problems related with information security, and are the ISO 17799 and ISO 27001. Those standards don't solve existent problems, but they help to avoid them. We should explain that those standards don't work alone, the institutions have much more work to do! Another measure taken to fight crimes related to information security is the adoption of legal instruments specially created by governments.

Palavras-chave

Segurança da Informação - Ameaças à Segurança da Informação - Protecção da Segurança da Informação

Introdução

O presente trabalho é realizado no âmbito da unidade curricular de Preservação e Conservação da Informação, leccionada pela Prof. Doutora Manuela Pinto, e tem como objectivo traçar uma perspectiva acerca da Segurança da Informação. Começando por uma abordagem mais primitiva ao tema, começar-se-á por tentar perceber porque surgiu a necessidade de segurança da informação, ao longo dos tempos. Trata-se de compreender o que é a segurança da informação, para que serve, quais os seus princípios e critérios, de que forma afecta ou condiciona as tomadas de decisão. Far-se-á também uma pequena abordagem à questão da segurança da informação a um nível governamental (segurança nacional relacionada com a segurança da informação).

Com a emergente era da informação, são cada vez mais e mais preocupantes as ameaçam à segurança da informação. Embora seja um pensamento comum atribuir-se a segurança da informação (ou a falta dela) à área estritamente tecnológica, não pode ou não deve ser esquecida a vertente humana e social.

Há mecanismos de combate, que permitem "agir" contra as falhas na segurança da informação que compreendem ferramentas de foro tecnológico, as chamadas Tecnologias de Segurança da Informação.

Será também feita uma referência às normas ISO relacionadas com a segurança da informação, as normas ISO 17799, ISO 27000 e ISO 27001.

A norma ISO 17799, fornece um plano que permite identificar e aplicar soluções para alguns riscos que envolvem a política de segurança, organização da segurança, classificação e controlo dos bens, controlo de acesso, contratação, formação e sensibilização para a segurança,

segurança física e ambiental, gestão de comunicações e operações, desenvolvimento e manutenção dos sistemas.

Quanto à norma ISO 27000, pertencendo à grande família das normas ISO, a norma ISO 27000 está directamente relacionada com a segurança da informação, mais concretamente com as tecnologias de segurança, uma vez que regula as técnicas de segurança da informação.

No que respeita à norma ISO 27001, é uma norma que deve ser combinada com a acima referida norma ISO 17799, tratando-se de um padrão direccionado para a gestão de segurança da informação.

Serão aqui também referidas algumas políticas de segurança da informação, compreendendo os métodos de avaliação, os mecanismos de partilha da segurança da informação, bem como alguns meios de combate ao *cibercrime*.

É também importante referir a importância do investimento em segurança da informação e da utilização de sistemas de segurança da informação.

Como último tópico (mas nem por isso menos importante), abordar-se-á também o tema da certificação digital[1].

Capitulo 1: Estrutura (pontos a abordar)

Far-se-á neste capítulo, uma pequena apresentação de todos os pontos que compõem esta análise, bem como uma pequena síntese do abordado em cada um desses pontos. É feita também uma resenha das fontes bibliográficas utilizadas, também em cada um desses pontos.

Estrutura

Uma vez que o que se pretende é abranger uma vasta série de sub-tópicos (relacionados com a Segurança da Informação), optou-se por dividir-se o tema pelos tópicos/capítulos a seguir enumerados:

1. **Estrutura (pontos a abordar):**
   É o presente capítulo, onde se procede à apresentação da estrutura do trabalho.
2. **Segurança da Informação (aspectos a considerar):**

Aqui questiona-se que na emergente era da Informação, a Segurança da Informação é cada vez mais uma preocupação para as organizações, uma vez que é exposta a um grande número de ameaças e vulnerabilidades, devendo ser continuamente protegida (ISO. **17799,** 2005). Procede-se a um enquadramento teórico, abordando essencialmente aspectos ligados ao facto de a Segurança da Informação da Informação estar naturalmente enquadrada na Inter-disciplina Ciência da Informação estando directamente inserida na área da Preservação e

[1] Note: ao longo da apresentação do trabalho não será necessariamente seguida a ordem referida aqui na introdução

Conservação da Informação, que por sua vez tem uma relação directa com as três áreas axiais de Ciência da Informação. Regendo-se pelos princípios básicos da *confiabilidade*, *autenticidade e integridade* da informação, a Segurança da Informação propõe-se reduzir os riscos de violação/destruição da informação nas organizações.

3. Ameaças à Segurança da Informação:

Apontam-se algumas ameaças de vária ordem à Segurança da Informação, desde as catástrofes naturais e humanas até aos ataques tecnológicos, não esquecendo a engenharia social.

Muitas vezes o perigo está dentro das próprias organizações. Questão como a Engenharia Social, que é também uma forte ameaça à Segurança da Informação…

4. Garantir a Segurança da Informação

Neste capítulo procura-se dar resposta aos problemas detectados na fase anterior, ou pelo menos dar sugestões para evitar esses problemas. Versando sobre os mecanismos tecnológicos será analisado o artigo *Managing Your Security Future*, em que o autor apresenta um panorama das actuais ameaças tecnológicas à Segurança da Informação, fornecendo de seguida um leque de respostas (também elas tecnológicas), a essas ameaças. Por sua vez, o autor do artigo *The Top Management Information Security Issues Facing Organizations: What Can Governments do to Help?* mostra-nos um estudo com a pretensão de determinar os principais problemas relacionados com a segurança da informação nas organizações, apresentando de seguida sugestões de apoios governamentais.

Serão abordados aspectos relativos à Certificação Digital.

Com o objectivo de apoiar as organizações na prevenção contra incidentes relacionados com a Segurança da Informação, são aqui analisadas as duas Normas ISO, a Norma ISO 17799, que é no fundo um conjunto de práticas para gerir a Segurança da Informação, (ISO 17799, 2005) , e a Norma ISO 27001 (ISO 27001,2005), de extrema importância para o tema.

Procurando consultar a opinião de um especialista sobre estas duas Normas, de um modo particular sobre a Norma ISO 27001, será consultado o artigo *ISO/IEC 27001 na opinião de um especialista*, da autoria de Francesco de Cicco. Não querendo deixar de parte a influência dos governos na protecção da Segurança da Informação, este ponto será também abordado, contando para isso com a analise dos artigos, (Knapp, K; Marshall, T.; JR. Rainer, R. K., et al.(2006).; Yoo, Don-Young; Shin, Jong-Whoi; Lee, Gang-Shin, et al. (2007).; Ott, J. L., 2000.), no primeiro artigo mencionado, são apontadas medidas que devem ser levadas a cabo pelos governos para proteger a Segurança da Informação nas organizações, por sua vez, o autor do segundo artigo apresenta-nos algumas medidas governamentais já tomadas e é apresentado também o National Information Infrastructure Protection Act, que é depois tratado de forma mais pormenorizada no último artigo referido.

Foi também encontrada alguma matéria que permitiu aplicar os temas da avaliação da segurança da informação e da importância da partilha de informação sobre os ataques.

Rol de fontes bibliográficas usadas em cada um dos capítulos

Agora, por ordem alfabética, apresentam-se as correctas referências bibliográficas, e de novo de acordo com os vários tópicos (a seguir a este: capítulos 2, 3 e 4) do trabalho, as fontes consideradas mais relevantes para levar a bom termo a abordagem a este tema:

Capítulo 2:

- Departamento de Ciência da Informação, C. d. C. J. e. E., UFES - Universidade Federal do Espírito Santo; and F.-F. d. L. d. U. d. P. Secção Autónoma de Jornalismo e Ciências da Comunicação Ciência da Informação. Dicionário Electrónico de Ciência da Informação.
- ISO (2005). ISO 17799. Suíça, ISO. **17799**.
- Laureano, M. A. P. (2005) Gestão de Segurança da Informação. 132
- Reed, B. (2007). "Implementing Information Lifecycle Security." Information Security Journal **16**(3): 5.

Capítulo 3:

- "Resultado! Concursos Notícias e Editais de Concursos Públicos 2010 – Provas, Gabaritos, Apostilas, Resultados e mais." 2010.;
- (2009). "Guia Prático para a Internet e as Novas Tecnologias." Internet e Novas Tecnologias: 16.
- C. G. d. "Glossário de Segurança." 2010, from http://www.cgd.pt/Seguranca/Glossario/Pages/Seguranca-Glossario.aspx.;
- Leitão, H. F. (2008) O perigo vem de dentro. Fuga de Informação ou Desinformação **36**;
- Lynch, D. M. (2006). "Security Against Insider Attacks." Information Security Journal **15**(5): 9.
- Reinhold, C.; Frolick, M.; Okunoye, A.(2009). "Managing Your Security Future." Information Security Journal **18**(3): 8.;

- Thompson, Samuel T. C. "Helping the Hacker." *Information Tecnology & Libraries* 25, no. 4 (2006): 5.

Capítulo 4:

("CERT: Organizational Security." 2010, from http://www.cert.org/work/organizational_security.html;

- ISO (2005). ISO 17799. Suiça, ISO. **17799**.;
- ISO (2005). ISO 27001. Suiça, ISO. **27001**.;
- Cicco, F.(2006)ISO/IEC 27001 na opinião de um especialista.3

• Yoo, Young-Dong; Shin, Whoi-Jong; Lee, Shin Gang, et al. (2007). "Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)." PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY(2007). "Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)." PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY: 6.;

- Khansa, Lara; Liginlal, Divakaran"Quantifying the Benefits of Investing in Information Security." Communications of the Acm **52**(11): 6.;
- Knapp, K; Marshall, T.; JR. Rainer, R. K., et al.(2006). "The Top Information Security Issues Facing Organizations: What Can Government Do to Help?" Information Security Journal **15**(4): 8;
- Multicert. "Certificados digitais." 2010, from https://www.multicert.com/certificadosdigitais.;
- Reinhold, C.; Frolick, M.; Okunoye, A.(2009). "Managing Your Security Future." Information Security Journal **18**(3): 8;
- Ott, J. L. (2000). "Information Security in the New Millenium." Information Security Journal **9**(1): 3.
- Republica, A. d. (2009). Lei 109 de 2009, Assembleia da República**:** 7.
- Thompson, Samuel T. C. "Helping the Hacker." *Information Tecnology & Libraries* 25, no. 4 (2006): 5.;.

Capitulo 2: Segurança da Informação (aspectos a considerar)

1 Segurança da Informação

Informação é um bem, que tal como outros bens relevantes, é essencial para as áreas de negócio de uma organização e precisa de ser constantemente protegida. Isto é especialmente importante na crescente inter-relação dos ambientes de negócio. Como resultado deste aumento de inter – conectividade, a informação é exposta a um número cada vez maior e mais variado de ameaças e vulnerabilidades.

A informação pode assumir várias formas. Pode ser impressa ou escrita em papel, armazenada electronicamente, transmitida através de meios electrónicos, através de filmes, ou falada. Seja qual for a forma assumida pela informação, ou o significado a partilhar ou armazenar, deve sempre proceder-se a uma protecção adequada.

A Segurança da Informação é a protecção da informação relativamente a um largo número de ameaças, com o objectivo de assegurar a continuidade do negócio, minimizar os riscos, e maximizar o retorno dos investimentos, bem como as oportunidades de negócio[2].

2 Enquadramento teórico

Antes de tudo, é importante proceder a um enquadramento teórico que torne perceptível o lugar ocupado pela Segurança da Informação na Ciência da Informação[3]. Todavia, inserindo-se a segurança da informação na chamada Preservação e Conservação da Informação, para se conseguir situar a Segurança da Informação na Ciência da Informação, é necessário fazer uma contextualização prévia da Preservação e Conservação da Informação. A Preservação e Conservação da Informação está integrada no ciclo da Gestão da Informação e tem uma relação de dependência directa com duas outras árias axiais de Ciência da Informação, o Comportamento Informacional e a Organização e Representação da Informação.

À luz do actual paradigma Científico/Informacional, a Preservação da Informação assume como desafios particulares: focar-se na informação e no processo Info-Comunicacional, sendo este um dos pontos que estabelece a relação de dependência directa com o Comportamento Informacional; encarar o dinamismo da Informação e do Processo Info-Comunicacional; no que respeita ao objecto digital, trabalha para assegurar a característica da

---

[2] *In* ISO (2005). ISO 17799. Suiça, ISO. **17799**.

[3] *In* Departamento de Ciência da Informação, C. d. C. J. e. E., UFES - Universidade Federal do Espírito Santo; and F.-F. d. L. d. U. d. P. Secção Autónoma de Jornalismo e Ciências da Comunicação Ciência da Informação. Dicionário Electrónico de Ciência da Informação.

multidimensionalidade, tendo as dimensões física e lógica como o suporte para a dimensão conceptual, como surgem cada vez mais ambientes de multiprodução da informação, a Preservação e Conservação da Informação vê também a resolução desse problema como um desafio.

A Preservação e Conservação da Informação pode ser entendida como um ciclo, que tem como ponto de partida a criação de uma plataforma tecnológica que potenciará a produção, armazenamento, recuperação, avaliação e utilização da informação. Avançar para um novo modelo de preservação e caso haja necessidade, construir, um novo tipo de operacionalização compreendendo todos os intervenientes.

Ao falar-se de Segurança da Informação, não seria lógico abordar-se em primeiro lugar uma definição de Informação? Talvez, no entanto, afigurou-se ser mais coerente fazê-lo agora, até porque, como se verá, a própria definição de Informação conduz à relação existente entre a Preservação e Conservação da Informação e o Comportamento Informacional. Em Ciência da Informação, a Informação é encarada não só do ponto de vista científico – que define Informação como um conjunto estruturado de representações mentais e emocionais modeladas e codificadas através da interacção social, e que podem ser registadas em qualquer suporte material – mas também como um fenómeno humano e social, também chamado de fenómeno Info-Comunicacional, estabelecendo aqui um elo de ligação com a área axial de Ciência da Informação Comportamento Informacional.

Agora é altura de questionar: qual a relação entre o processo Info-Comunicacional e a Preservação e Conservação e mais concretamente com a Segurança da Informação? A resposta é…tudo. A informação enquanto parte integrante do processo Info-Comunicacional é composta por vários passos, desde a concepção e criação da informação até á sua interpretação, incluindo o seu armazenamento e divulgação, pesquisa, etc., e ao longo de todos estes passos é necessário preservar a informação.

Embora a informação ao nível material ou físico, (por exemplo livros no seu conceito tradicional) ainda seja uma realidade influente, assistimos a uma cada vez maior proliferação da produção da informação em formato digital. O objecto digital é composto por várias dimensões que embora distintas são interdependentes, são elas: **Dimensão física**: esta dimensão compreende o suporte físico da informação, que pode, e muitas vezes está a quilómetros de distância da pessoa que está a utilizar a informação. Como exemplos de suporte físico temos: CDs, Pendrives, Discos Rígidos, etc., para além do suporte físico existe ainda o software, que, também condiciona muito a informação produzida; a **Dimensão lógica**: a dimensão lógica compreende o código utilizado para produzir informação, código que tem de ser passível de ser interpretado por um computador; a **Dimensão Conceptual**: aqui está patente o significado que o individuo que produz e/ou lê a informação atribui ao código utilizado, fazendo assim uma interpretação personalizada desse mesmo código; e a **Dimensão essencial**: esta ultima

dimensão, mas nem por isso a menos importante, diz respeito ao conteúdo da mensagem, ao código e aos caracteres utilizados, uma vez que tem como meta determinar/avaliar a relevância da mensagem para verificar se é justificável a sua preservação. Por exemplo: que tipo de informação será mais importante preservar: uma conversa de circunstância no *msn*[4]…ou um ficheiro recebido com o nosso extracto bancário? Em qual destes casos seria mais prejudicial a deterioração ou até mesmo violação da informação? Como se relacionam entre si as varias dimensões? Todas as dimensões que compõem o objecto digital estão intimamente relacionadas, senão vejamos: embora o código utilizado na dimensão lógica não esteja necessariamente vinculado a um suporte físico específico está dependente do tipo de suporte utilizado. Por sua vez o conteúdo/significado da informação (dimensão conceptual) tem uma relação directa com os caracteres ou código utilizado, e por último, a dimensão essencial – como já foi previamente referido – está intimamente relacionada com todas as outras dimensões.

Sob o ponto de vista da Ciência da Informação, a Preservação da Informação em formato digital é feita em dois níveis: a nível estratégico e de gestão, e a nível operacional. O nível estratégico e de gestão compreende: a Introdução de políticas e medidas que permitam gerir a preservação da informação, zelando pela sua segurança; a utilização de ferramentas normativas e legais, através das quais seja possível não só proteger/preservar a informação, mas também punir infractores; a instituição de órgãos que procedam à criação dessas ferramentas normativas e legais e zelem pelo seu cumprimento; a criação de regulamentos internos às próprias instituições que pretendam preservar a informação. A nível operacional basicamente é colocar em prática as medidas definidas no nível estratégico e de gestão, implementar acções que visem proteger a informação, acções que devem ser realizadas no âmbito do Sistema de Informação implementado.

Em suma, o objectivo da preservação do objecto digital é garantir que este é fidedigno, autentico, íntegro, e acessível a longo termo.

Como é perceptível, é deveras importante a utilização de Normas ou Padrões Internacionais, e Protocolos. Em primeiro lugar a adopção de normas ou padrões internacionais permite evitar algumas situações de risco ou de violação da informação. A questão dos Protocolos está directamente relacionada com o estabelecimento de relações de cooperação com industrias de tecnologia, de forma a potenciar a compra e a expansão de sistemas electrónicos de gestão da informação, conciliados com a legislação em vigor e com a gestão da informação.

É igualmente importante não esquecer a meta-informação e consequentemente definir estruturas normalizadas que permitam gerir o acesso e a preservação do objecto digital. Qual o melhor procedimento para assegurar a Segurança da Informação Digital? Para além de tudo o que já foi mencionado, as organizações devem instituir uma política de segurança da informação

[4] ***Msn***: Messenger é um programa das mensagens instantâneas criado pela Microsoft Corporation.

de acordo com a sua cultura organizacional, informacional, bem como as questões humanas e tecnológicas. Ao proceder assim assegurará a confidencialidade da informação, a sua autenticidade e segurança, daí a sua relação com a gestão da informação.

Após tudo isto, acredita-se ser possível perceber a importância da segurança da informação no ciclo de vida da informação e consequentemente no âmbito da ciência da informação.

A segurança da informação pode pois, e deve ser avaliada em termos físicos e em termos lógicos: a **segurança física** compreende, como o próprio nome indica, as ameaças físicas, como: incêndios, desabamentos, relâmpagos, inundações, acesso indevido de pessoas, forma inadequada de manuseamento e tratamento do material, etc.

Quanto à **segurança lógica**, atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, backups desactualizados, violação de palavras-chave, etc..

Através de todas estas dimensões entra em acção a terceira área axial de Ciência da Informação mencionada, a Organização e Representação da Informação. Agora coloca-se uma questão: de que forma a Organização e Representação da Informação está relacionada com a pluridimensionalidade do objecto digital? Ao longo das quatro dimensões do objecto digital verifica-se a presença de meta-informação, uma vez que para se produzir informação é necessário utilizar códigos apenas inteligíveis por computador (o que é o mesmo que dizer que a informação se produz a partir de informação, ou seja: a partir de código informático é produzida informação inteligível para o leitor e para o utilizador). Para alem disso, na dimensão essencial é necessário organizar e representar a informação resultante de todas as outras dimensões – suporte físico e digital (software) utilizado, caracteres, e significado da informação – para determinar se, se justifica ou não a preservação dessa informação.

1.1 A importância da Informação

A informação tem um valor altamente significativo e pode representar grande poder para quem a possui.

No âmbito da Ciência da Informação trans e interdisciplinar defende-se que tem uma dupla funcionalidade semântica. Refere um fenómeno humano e social que compreende tanto o dar forma a ideias e a emoções (informar), como a troca, a efectiva interacção dessas ideias e emoções entre seres humanos (comunicar). E identifica um objecto científico, a saber: conjunto estruturado de representações mentais e emocionais codificadas (signos e símbolos) e modeladas com/pela interacção social, passíveis de serem registadas num qualquer suporte material (papel, filme, banda magnética, disco compacto, etc.) e, portanto, comunicadas de forma assíncrona e multi-direccionada. Um objecto científico assim concebido demarca-se claramente da tendência que se foi generalizando, a partir de meados de novecentos, de espalhar

o conceito da imprensa à biologia e das definições que se multiplicaram sob a égide da teoria matemática da transmissão de sinais, genérica e abusivamente conhecida por teoria da informação, de *Shannon* e *Weaver*, não obstante todo um esforço feito para aplicá-la com proveito no campo das Ciências Sociais e mais especificamente na ciência da comunicação. Mas, como advertiu, implicitamente, *Anthony Wilden* a dimensão simbólica e humana do conceito Informação não é redutível à dimensão física e quantitativa, à qual se refere a teoria de Shannon. Relacionar a existência de informação com a redução da incerteza não permite captar a complexidade introduzida pelas ambiguidades do sentido e da interpretação que estão no âmago do fenómeno info-comunicacional.

Vivemos numa sociedade que se baseia em informação e que exibe uma crescente propensão para obter e armazenar informação e o uso efectivo da informação permite que uma organização aumente a eficiência de Operações segundo *Katzam*, 1977.

A informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade (*Rezende e Abreu, 2000).*

As empresas já perceberam que o domínio da tecnologia como aliado para o controlo da informação é vital. O controlo da informação é um factor de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial já o defendiam *Synnat*, 1987; *Feliciano Neto, Furlan e Higo*, 1988. Dispor da informação certa, na hora certa, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos dados e sistemas, a informação ganhou mobilidade, inteligência e real capacidade de gestão[5].

1.2 Princípios de Segurança da Informação

A segurança da informação busca reduzir os riscos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informação ou qualquer outra ameaça que possa prejudicar os sistemas de informação ou equipamentos de um indivíduo ou organização.

Segundo P*UTTINI* (2001), uma solução de segurança adequada deve satisfazer os seguintes princípios:

---

[5] *In* Departamento de Ciência da Informação, C. d. C. J. e. E., UFES - Universidade Federal do Espírito Santo; and F.-F. d. L. d. U. d. P. Secção Autónoma de Jornalismo e Ciências da Comunicação. Dicionário Electrónico de Ciência da Informação.
In Laureano, M. A. P. (2005) Gestão de Segurança da Informação. 132

A ***confiabilidade***, que significa proteger informação contra a revelação para alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida. Deve-se cuidar não apenas da protecção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas ou capturados por dispositivos ilícitos.

A ***autenticidade***, o controlo de autenticidade está associado com a identificação correcta de um utilizador ou computador. O serviço de autenticação de um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada no seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo o processo de identificação, seja de um utilizador para um sistema, de um sistema para o utilizador ou de um sistema para outro sistema. Ela é a medida de protecção de um serviço/informação contra a personificação por intrusos.

A ***integridade***, consiste em proteger a informação contra a modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui acções como escrita, alteração de conteúdo, alteração de status, remoção e criação de informação. Deve-se considerar a protecção da informação nas suas mais variadas formas, como por exemplo, armazenada em discos ou fitas de *backup*. Integridade significa garantir que se o dado está lá, então não foi corrompido, encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado. A integridade é assegurada evitando-se alteração não detectada da mensagem.

A ***disponibilidade***, que consiste na protecção dos serviços prestados pelo sistema de forma a, que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao utilizador o acesso aos dados sempre que deles precisar.

Através da correcta aplicação destes princípios, a segurança da informação pode trazer benefícios como o aumento da produtividade dos utilizadores através de um ambiente mais organizado, maior controlo sobre os recursos de informática e garantia da funcionalidade das aplicações críticas de uma empresa.

De uma forma coerente estes princípios vão de encontro ao que ocorre no fenómeno info-comunicacional e consequentemente à visão da informação como um processo. Ou seja, o fenómeno info-comunicacional versa sobre a comunicação da informação e consequentemente isso requer que esta esteja disponível, pode ou não ser confidencial, e/ íntegra.

1.3 O Ciclo de Vida da Segurança da Informação

Tal como John Oltsik[6], defende-se que também a segurança da informação tem um ciclo de vida que as organizações devem zelar para que seja cumprido. Segundo este autor, o ciclo de vida da segurança da informação compreende nove etapas chave, são elas: 1- Classificação de dados: Classificar os dados de acordo com as políticas vigentes n ciclo de vida da informação e da própria organização, para determinar como a informação será monitorizada; 2- Fluxo de informação: Classificar e localizar os movimentos e as modificações da informação com base na alteração de dados; 3- Acesso à informação: Mapear o acesso à informação de acordo com a classificação dos dados; 4- Utilização da informação: Uma componente de gestão digital baseada na classificação de dados; 5- Gestão de risco da informação: A segurança da informação e a protecção de dados são baseadas na classificação de dados; 6- Políticas de funcionamento do ciclo de vida da segurança da informação: Depois da classificação de dados existem regras que regem os dados tal como os fluxos e as alterações; 7- Classificadores e repositores de metadados: Classificar a informação através de um conjunto de regras e dotando-a de uma identidade passível de ser universalmente compreendida; 8- Sistemas de ficheiros seguros: Distribuir sistemas de ficheiros que reconheçam e interajam com diferentes políticas de conduta, identidades de informação e metadados; 9- Gestão centralizada: Se o armazenamento de informação tiver de seguir algum conjunto de regras ou contiver um repositório de metadados, deverá ter também um registo centralizado da informação

[6] *In* Reed, B. (2007). "Implementing Information Lifecycle Security." Information Security Journal **16**(3): 5.

Capítulo 3: Ataques à Segurança da Informação

2 Ameaças à Segurança da Informação

2.1 Os incidentes naturais e humanos e a destruição da informação

Incidentes como: roubos, guerras, inundações, incêndios, podem colocar em risco a segurança da informação. O exemplo que se segue versa sobre um incêndio na Biblioteca de Anna Amalia em Weimar e demonstra o quão prejudicial este elemento se pode tornar para a segurança da informação. O incêndio na biblioteca Anna Amalia, em Weimar, causou danos irreparáveis ao legado literário alemão. O local, que abrigava livros raros, havia sido declarado património da humanidade pela Unesco. Estima-se que cerca de 30 mil obras dos séculos 16, 17 e 18 tenham sido destruídas. Outros 40 mil livros foram sériamente danificados pela acção do fumo e da água usada para apagar o fogo, muitos deles de valor inestimável, como a colecção de 3900 volumes da obra *Fausto*, de *Johann Wolfgang Von Goethe*, 2 mil pergaminhos medievais, 8400 mapas históricos, 500 manuscritos do filósofo *Friedrich Nietzsche* e ainda uma colecção de bíblias, incluindo a bíblia de *Martinho Lutero*, de 1534, que foi salva com ajuda da população. Tudo leva a crer que o fogo tenha sido desencadeado por um defeito na parte eléctrica. Apesar de todos os esforços, não foi possível salvar todo o acervo. Toda a valiosa colecção de livros musicais, que estava na sala principal, foi queimada pelo incêndio. Era uma das 12 bibliotecas mais importantes da Alemanha. O espaço, que abrigava obras de Schiller, Herder e Wieland, por exemplo, era considerado "berço do classicismo alemão". Ironicamente, o incêndio na biblioteca aconteceu cinco semanas antes de o acervo ser transferido para outro lugar justamente para que o castelo pudesse ser restaurado e modernizado[7].

Ilustração 2 Sala da biblioteca Anna Amalia

Ilustração 1 Incêndio na Biblioteca de Weimar

Também a famosa biblioteca de Florença foi parcialmente destruída em 1966, desta feita através da água, uma vez que foi inundada pelo rio *Arno*, inundação, que causou uma

[7] *In* (2004). Incêndio destroi património da humanidade. DW-WORLD. DE, B2B.

destruição incalculável do acervo da biblioteca. Mas as inundações não são apenas provocadas pelo vazamento dos rios, podem ser também causadas por: estragos nas janelas ou nos telhados, pelo próprio combate aos incêndios, obstrução de caleiras, infiltrações, canalizações rompidas, rompimento das condutas de aquecimento central ou ar condicionado, etc..

Em Colónia, em 2009, a fachada principal da Biblioteca sofreu uma devastadora derrocada, causando a destruição de uma grande parte do seu acervo.[8]

2.2 Fuga de informação

Em português comum podemos designar fuga de informação, como o acesso, divulgação de informação privada e supostamente protegida e interdita. Face a este problema, as empresas investem cada vez maiores quantias de dinheiro em tecnologia informática que visa barrar o acesso à informação dita privada da organização. Todavia, nem sempre a fuga de informação é feita através dos meios informáticos, e há uma certa tendência para esquecer o meio social e humano. Pois é, os maiores desvios da informação surgem a partir do interior da própria empresa, pela mão dos seus colaboradores. Note-se que esse desvio da informação pode ser feito tanto de forma consciente como inconsciente. Muitas vezes, as pessoas servem-se da chamada 'Engenharia Social', para apelar ao sentimentalismo e à boa vontade dos colaboradores, induzindo-os – de forma inconsciente para estes – ao fornecimento de informação supostamente sigilosa ou confidencial. Também a tecnologia informática pode ser posta ao serviço da 'Engenharia Social', através do envio de emails maliciosos, os típicos emails que pedem para o destinatário clicar em algum *link* com o suposto objectivo de abrir uma imagem ou um documento, mas cujo objectivo real é abrir o acesso dos computadores da organização ao individuo invasor.

Voltando á faceta social e humana, um erro em que as organizações tendem a cair é tornar visíveis a todos os colaboradores, as informações consideradas privadas ou sigilosas para a organização, deixando assim, ao critério dos colaboradores, a devida ou indevida utilização da informação[9].

2.3 Engenharia Social

De acordo com o Instituto de Gestão e Administração IOMA, a Engenharia Social foi vista como a principal ameaça à segurança no ano de 2005. E o que é a Engenharia Social? A

---

[8] *In* Pinto, M. M. (2010). Apoio a Aulas 3**:** 96.

[9] *In* Leitão, H. F. (2008) O perigo vem de dentro. Fuga de Informação ou Desinformação **36**, 2

Engenharia Social é um método que tem como objectivo obter acesso a informação ou a sistemas de computação interditos. Baseia-se na obtenção de informação privada a partir da persuasão, manipulação emocional, abuso de confiança e impersonalização, técnicas utilizadas pelo engenheiro social para com um colaborador de determinada organização. É uma técnica que funciona porque se apoia na honestidade e inocência das vítimas, que partem do princípio que esses valores também são aplicáveis à outra pessoa (engenheiro social).

Tratando-se de alguém muito semelhante ao Hacker, o Engenheiro Social é também apelidado de Hacker não técnico, uma vez que não se apoia na utilização de tecnologia informática para obter as informações pretendidas. Como já foi subliminarmente referido, o Engenheiro Social é dotado de um verdadeiro arsenal de armas psicológicas que apontadas à vítima de forma eficaz, levam à obtenção da informação desejada, sem que sejam necessários processos muito rebuscados. Muitas vezes a informação é pedida de forma directa, e como já também foi referido, através de uma enorme capacidade de transmissão de confiança e da manipulação emocional da vítima.

Em muitos casos de apelo de confiança e de manipulação emocional da vítima, o engenheiro social pode por exemplo vestir a pele de um técnico informático, e manipular o utilizador final de um computador dirigindo-se a sua casa e insinuando que algo está a funcionar mal no computador, pede ao utilizador que lhe forneça algumas informações para corrigir o suposto problema. Apreciando a preocupação e a assistência, a vítima fornece as informações sem se aperceber da falta de carácter do suposto técnico.

Outra arma muito utilizada é a manipulação de simpatia. É muito utilizada por indivíduos fornecedores de informação, como por exemplo colaboradores de helpdesk. Aqui, o engenheiro social contacta a vítima e afirma que necessita de uma informação que deveria ter e não tem, e de novo, acreditando nas boas intenções da pessoa que pediu a informação, a vítima fornece-a sem colocar quaisquer reservas.

Uma outra técnica, a impersonalização, está relacionada com a necessidade de conquistar a confiança da vítima e de para isso o engenheiro social se fazer passar por alguém que seja uma outra pessoa, ou por alguém que tem uma outra profissão, adequada ao tipo de informação que ele/ela pretende obter. Com esta técnica, o engenheiro social tem também (para além da obtenção da informação), como principal objectivo conquistar a confiança da vítima. A pesquisa é outra técnica utilizada pelo engenheiro social, pois permite-lhe descobrir que informação deve pedir, como as deve pedir e a quem as deve pedir[10].

---

[10]*In* Thompson, Samuel T. C. "Helping the Hacker." *Information Tecnology & Libraries* 25, no. 4 (2006): 5.

2.4 Tecnologias da Informação

Com a integração da Internet no quadro comunicacional de grande parte das organizações, assistiu-se à invasão de uma multiplicidade de técnicas, métodos ou mecanismos de software malicioso que surgiram com o intuito de violar a informação, e mais alarmante ainda é o facto da grande maioria dos *ciber-ataques* a seguir descritos terem origem no interior das organizações. Não existe nenhuma técnica cem por cento eficaz para traçar o perfil de um potencial atacante. Pelo contrário, o seu perfil indica-o como um vulgar colaborador de qualquer organização moderna, o atacante pode desempenhar qualquer função na organização, desde programador, artista gráfico, gestor de rede, etc. são no fundo colaboradores que tendo autorização para utilizar os Sistemas de Informação da organização, fazem-no com fins ilícitos[11].

Os peritos Kenneth J. Knapp, Thomas E. Marshall, R. Kelly Rainer, Jr., e Dorsey W. Morrow desenvolveram um estudo descrito no artigo[12] *Top Information Security Issues Facing Organizations: What Can Government do to Help?* e não deixa de ser curioso o facto de após uma análise aos resultados deste estudo se perceber que ao contrário do que inicialmente se pensava, as questões de *malware* não pertencem sequer aos dois problemas mais preocupantes, ocupando uma modesta terceira posição, sendo superados por problemas relacionados com a falta de preparação e de consciencialização dos utilizadores relativamente aos *ciber-ataques* e ainda mais pela falta de apoio à gestão de topo.

Seguem-se alguns exemplos de ataques relacionados com o malware e com o cibercrime:

2.4.1 Hacker

É um indivíduo que ilegalmente tenta entrar em sistemas informáticos, sendo normalmente um bom programador, que através de bons conhecimentos tecnológicos tenta furar a segurança de sistemas informáticos tipicamente classificados como seguros, através da identificação e exploração dos pontos fracos desses sistemas[13].

2.4.2 CiberCrime

Denominação atribuída aos crimes cometidos através da Internet, são vários os exemplos de *CiberCrimes*, desde o desvio de dinheiro de contas bancárias; acesso, modificação

---

[11] *In* Lynch, D. M. (2006). "Security Against Insider Attacks." Information Security Journal **15**(5): 9.

[12] *In* Knapp, K; Marshall, T.; JR. Rainer, R. K., et al. (2006). "The Top Information Security Issues Facing Organizations: What Can Government Do to Help?" Information Security Journal **15**(4): 8.

[13] *In* Depósitos, C. G. d. "Glossário de Segurança." 2010, from http://www.cgd.pt/Seguranca/Glossario/Pages/Seguranca-Glossario.aspx.

e violação de dados interditos; roubos através de cartões de crédito, violações de propriedade intelectual, pedofilia, etc.

2.4.2.1 Adware

Programas que são instalados com o objectivo de recolher dados pessoais de utilizadores, utilizando para isso a fachada de anúncios publicitários na internet.

2.4.2.2 Cracker

Pessoas que invadem e desviam informação pertencente a outros.

2.4.2.3 Pharming

Trata-se de um ataque informático que altera a ligação existente entre um website e um servidor Web, para que os pedidos de acesso a um site sejam enviados para um outro endereço controlado por/pelos individuo(s) "atacantes".

2.4.2.4 Phishing

É uma técnica utilizada com objectivo de extrair informação dos utilizadores, através da criação de páginas web falsas em tudo similares às verdadeiras.

2.4.2.5 Spyware

Programas informáticos, que sub-repticiamente instalados nos computadores dos utilizadores, registam todas as acções destes, registando tudo o que é digitado no computador e/ou armazenando as páginas Web visitadas, encaminhando esses dados para o computador da pessoa que instalou o programa.

2.4.2.6 Outros tipos de ataque

Existem vários outros tipos de ataques à Segurança da Informação, alguns deles relacionados com o protocolo TCP/IP. Um famoso exemplo é o chamado ataque DOS, que consiste em sobrecarregar um servidor com demasiadas solicitações de serviços incapacitando o próprio servidor de internet. [14][15]

2.4.2.7 Vírus informáticos

2.4.2.7.1 O que são

Os vírus são programas que provocam danos intencionais no software e/ ou no hardware dos computadores. São normalmente formados pelas seguintes partes: *concealer* - parte que atribui ao vírus capacidades para que não seja detectado pelos programas anti-virus normais;

[14] *In* Okunoyea, C. R. M. N. F. A. (2009). "Managing Your Security Future." Information Security Journal **18**(3): 8.

[15] *In* "Resultado! Concursos
Notícias e Editais de Concursos Públicos 2010 – Provas, Gabaritos, Apostilas, Resultados e mais." 2010.

payload: é uma espécie de código programador do vírus que indica a finalidade ou o objectivo do próprio vírus, sendo que muitas vezes um vírus é dotado de múltiplos *payloads*.

Associados aos vírus normais existem os chamados *Worms*, que mais não são do que vírus muitos sofisticados, que têm a capacidade de auto-replicar automaticamente[16].

Para além dos *Worms* existem muitos outros tipos de vírus, desde os *Bankers* (destinados a roubo de informação bancárias), até aos *KeyLogger* que capturam informação digitada pelos utilizadores, passando pelos *Spyware*, que são programas clandestinos com a finalidade de roubar senhas, vigiando para isso o que é digitado nos computadores e as páginas de Internet acedidas pelos utilizadores transmitindo-as para o computador da pessoa que lançou o vírus.

2.4.2.7.2 Como se propagam:

Os vulgares vírus podem propagar-se de diversas formas, sendo as mais usuais através do envio e/ ou descarregamento de mensagens ou ficheiros contaminados. Por sua vez, um *worm* começa por determinar os pontos fracos nos computadores das vítimas, fazendo a sua invasão a partir desses pontos, depois transfere para esses computadores o código malicioso, procurando de seguida outros computadores ligados à mesma rede; activa o seu *payload*, e “infesta” o computador da vítima[17].

2.5 Caso prático

2.5.1 Vulnerabilidade das Bibliotecas (Segurança da Informação)

As bibliotecas são de facto instituições bastante vulneráveis no que respeita à Preservação e Conservação da Informação e consequentemente à Segurança da Informação. A prova disso é um inquérito realizado pela BAD[18], (que embora tenha sido realizado já em 1998, crê-se que infelizmente os seus resultados ainda são bastante actuais). A partir desse inquérito foi possível determinar que as bibliotecas públicas se debatem com inúmeros problemas para preservar e conservar os documentos - e por incrível que pareça, os documentos mais problemáticos são os livros modernos, devido à má qualidade do papel – seguindo-se as publicações periódicas (pelo mesmo motivo e também pelo facto de ser relativamente fácil para os leitores levar as publicações para casa, surripiar folhas ou partes de folhas, etc.). Para além disso, é elevado o número de bibliotecas que se encontram em edifícios que não foram construídos para essa finalidade, não estão bem localizados, não são dotados de equipamentos

[16] *In* (2009). "Guia Prático para a Internet e as Novas Tecnologias." Internet e Novas Tecnologias: 16.
[17] *In* (2009). "Guia Prático para a Internet e as Novas Tecnologias." Internet e Novas Tecnologias: 16.

[18] Associação Portuguesa de bibliotecários, arquivistas e documentalistas

que garantam uma maior protecção da informação em caso de desastre natural, como por exemplo portas corta-fogo.

Grande parte das bibliotecas estudadas estavam equipadas com estantes de madeira, o que representa um grande perigo em caso de incêndio. Também não deixa de ser alarmante que uma grande percentagem das instituições inquiridas não responderam ou não tem qualquer plano de emergência. Também se verificou uma grande percentagem de abstenção e/ou de inexistência de um plano de Preservação e Conservação de Informação, bem como da existência de um responsável por essa secção. Mas talvez isso seja justificável com a baixa disponibilidade de verbas para aplicar nessa área.

Quanto às condições ambientais, também aqui impera o aspecto negativo, uma vez que existe uma elevada taxa de bibliotecas que não procede ao controlo das chamadas condições ambientais. Quanto ao controlo dos fundos e das colecções, embora a maior parte das instituições inquiridas afirme controlar os fundos e as colecções que detém, existe ainda uma manifesta falta de controlo por parte das bibliotecas, o que propicia uma maior facilidade no desvio de documentos. De ressalvar ainda que uma grande fasquia das bibliotecas em estudo afirmaram não deter meios nem desenvolver acções com o objectivo de conservar a informação[19].

Todavia, as vulnerabilidades das bibliotecas não se limitam à informação material, nem tão pouco às obras, o facto das Bibliotecas possuírem bases de dados com os nomes, endereços, e dados pessoais sobre os seus utilizadores, torna-as num potencial alvo para os hackers e engenheiros sociais. Essa informação pode ser utilizada como um fim em si próprio, ou como um patamar para violar a segurança da informação noutros sistemas. Sendo muito dispendiosas as subscrições de propriedade de bases de dados, e sendo limitadas as licenças, o acesso a estes recursos de informação torna-se mais facilmente atingível para os hackers. Podem ser hackers casuais, que apenas pretendam obter acesso aos recursos da biblioteca para o seu próprio computador, ou podem ser *hackers* com um índice de criminalidade mais elevado, que roubam direitos de propriedade intelectual para um fornecedor de base de dados. Uma agravante para este problema é o facto de as bibliotecas terem acesso de banda larga a uma grande extensão de rede, banda larga essa que reúne a capacidade de fazer download de informação de outras redes, 'motivando' assim os *hackers* a utilizar este recurso para fins ilícitos, com ínfimas hipóteses de detecção.

A crescente automatização das bibliotecas também acaba por colocar em risco a sua segurança, uma vez que torna possível uma cada vez maior infiltração de *hackers* através da utilização de computadores remotos.

---

[19] *In* Pinto, M. M. (2010). Apoio a Aulas 2**:** 46.

Mas a vulnerabilidade das bibliotecas não está apenas relacionada com os hackers, sendo também, justificadamente incluídos os engenheiros sociais, pelas razões já mencionadas aquando da apresentação da engenharia social[20].

Capítulo 4: Garantir a Segurança da Informação

3 Mecanismos de protecção de Segurança da Informação

3.1 Protecção contra incidentes naturais e humanos

Existem uma série de regras que, sendo seguidas – embora não garantam uma protecção total da informação – ajudam a prevenir e contornar algumas vulnerabilidades das instituições no que se refere à protecção da informação.[21]

O roubo é uma ameaça constante que paira, como um fantasma em todas as instituições que detêm informação, todavia (embora nenhum método tenha uma taxa de eficácia de 100%), existem algumas regras que ao serem seguidas podem contornar consideravelmente algumas vulnerabilidades apresentadas pelas instituições são elas: conceber o edifício de forma a que os pontos de acesso (janelas, portas, elevadores, etc.), sejam apenas os estritamente necessários; equipar o edifício com um bom sistema de segurança; não facilitar o acesso de estranhos aos locais com acesso limitado aos colaboradores da organização; identificar devidamente os colaboradores e os utilizadores; proceder a uma actualização constante dos ficheiros que contêm a identificação dos leitores e dos colaboradores e mantê-los em segurança; manter os espaços públicos em vigilância constante; marcar as espécies para que a sua procedência possa ser correctamente identificada (tanto fisicamente como através dos sistemas de detecção magnéticos); se necessário proibir a entrada dos utilizadores com material susceptível de dissimular actos de roubo, como por exemplo sacos ou casacos; impulsionar a implementação de sistemas de alarme rigorosos que funcionem 24 horas por dia; manter um inventário actual das espécies existentes na instituição para controlar melhor o próprio acervo.

Para proteger a informação contra a guerra e catástrofes naturais deve-se: sempre que possível fazer uma previsão de potenciais ocorrências desses acontecimentos; proceder-se (sempre que necessário) a uma reestruturação arquitectónica dos edifícios, tendo sempre em linha de conta os potenciais danos causados pelo fogo ou pela água e por último, devem existir planos de emergência para a remoção e salvamento dos acervos.

---

[20] *In* Thompson, Samuel T. C. "Helping the Hacker." *Information Tecnology & Libraries* 25, no. 4 (2006): 5.

[21] *In* Pinto, M. M. (2010). Apoio a Aulas 3**:** 96

Para garantir uma maior protecção de informação em caso de incêndio deve ter-se em conta o seguinte: proceder à colocação de portas corta/fogo e manter os depósitos o mais afastados possível das instalações eléctricas; eliminar tanto quanto possível os espaços abertos, as grandes escadarias, pois funcionam como correntes que potenciam o alastramento dos incêndios; implementar saídas de emergência para os profissionais e utilizadores das instituições; seguir os requisitos legais aplicáveis a este tipo de questões; utilizar materiais não inflamáveis e não tóxicos; implementar sistemas de detecção de incêndios e alarmes actualizados; instalar sistemas eléctricos secundários que sejam uma alternativa aos sistemas eléctricos principais; verificar periodicamente: circuitos eléctricos, equipamento informático, equipamentos de extinção de incêndios, produtos químicos (em caso de existência de laboratórios e/ou oficinas); apostar na formação dos profissionais para enfrentar este tipo de riscos; delimitar espaços para fumadores…

3.2 Tecnologias de Segurança da Informação

São várias as tecnologias propositadamente criadas para proteger/garantir a segurança da informação na área computacional. Do Firewall às Biometrias, é colocado à disposição do utilizador um vasto leque de alternativas ou de medidas complementares que lhe permitem salvaguardar a informação.
Passemos então à definição de algumas dessas ferramentas:

3.2.1 Resposta a incidentes internos…

Como as mais sérias ameaças á segurança da informação são internas à própria organização, *David Lynch*[22] propõe a criação de uma espécie de perímetro que estabeleça a fronteira entre um interior fiável e um exterior que não expira confiança. Esse perímetro tem como função reforçar as medidas de controlo ao acesso da informação, isto baseia-se no conceito de confiança tribal, ou seja: "se pertences à minha tribo eu confio em ti…se não pertences essa confiança não existe". Transpondo isto para as organizações, pode definir-se que – *quem trabalha para a minha empresa é de confiança, quem não trabalha não é*. Há um elemento constante na grande maioria dos *ciber-ataques*, que é o facto de terem origem no interior da própria organização. O problema maior reside no facto desses ataques não serem casos isolados, muito pelo contrário, estarem a expandir-se perigosamente a uma escala global e serem fortemente impulsionados pela influência que a Internet exerce nos negócios.

[22] *In* Lynch, D. M. (2006). "Security Against Insider Attacks." Information Security Journal **15**(5): 9.

Para combater estes ataques internos têm sido tomadas medidas a vários níveis, desde reforços legais até ao desenvolvimento de software 'amigo', (como os exemplos a seguir demonstrados). Hoje em dia, nem o facto de que alguém está do lado de dentro do perímetro é sinónimo de que essa pessoa é confiável, e torna-se necessário recorrer às novas tecnologias para combater os ataques tecnológicos (como alias tem toda a lógica). É necessária a existência de tecnologia que, através das infra-estruturas existentes ajude as organizações a monitorizar as suas redes internas, definindo as permissões para os fluxos de informação e assegurando que a informação confidencial está sempre codificada. Tem de ser uma tecnologia capaz de cobrir toda a rede e assegurar um ambiente seguro, cumprindo para isso as seguintes etapas:

1 Estabelecer as necessárias relações de segurança;
2 Delimitar as redes internas às zonas seguras, de forma a serem facilmente geridas;
3 Reforçar a segurança das ligações estabelecidas através do cruzamento de zonas de segurança;
4 Fazer auditorias periódicas à rede interna para assegurar que é reforçada continuamente a segurança das redes existentes;
5 Gerir e actualizar as relações de segurança, encarando-as como qualquer outra necessidade de negócio;
6 Adoptar um sistema de auditoria e de relatórios periódicos.

Recomenda-se ainda que a Gestão de Topo se consciencialize da importância que a segurança da informação representa para a sobrevivência da própria organização. [23]

3.2.2 Firewall[24]

É um programa que controla o tráfego entre a Internet e uma rede interna, protegendo essa rede contra eventuais ataques de hackers informáticos, muitas vezes quando o firewall falha, essas falhas estão relacionadas com erros humanos – como por exemplo erros de configuração - e não com os próprios computadores[25];

3.2.3 Antivírus

É um programa utilizado para detectar a presença de vírus em computadores ou redes, eliminando-os, e actuando contra os efeitos nocivos causados pelo vírus, funciona também como uma barreira protectora contra novos ataques de vírus da mesma espécie[26].

[23] *In* Knapp, K; Marshall, T.; JR. Rainer, R. K., et al. (2006). "The Top Information Security Issues Facing Organizations: What Can Government Do to Help?" Information Security Journal **15**(4): 8.

[24] *In* "WebHouse.Net: Glossário de Termos da Internet." Retrieved 2010

[25] *In* Reinhold, C.; Frolick, M.; Okunoye, A. (2009). "Managing Your Security Future." Information Security Journal **18**(3): 8

[26] *In* "SANKHYA: Gestão de Negócios." from http://www.sankhya.com.br/glossario_a.php.

3.2.4 Anti spyware/ anti adware

São programas utilizados para evitar a penetração de programas espiões como programas de *Spyware* e de *Adware*.

3.2.5 Controlo de acesso pelos servidores

Basicamente é o controlo de acesso à informação privada, garantido pelo servidor de rede.

3.2.6 Detecção de Intrusões (sistema IDS)

Um sistema IDS é um sistema que tem como objectivo localizar e detectar intrusões.

É muito importante ter um sistema de Detecção de Intrusões seguro, uma vez que se algum hacker detectar um sistema de IDS numa determinada rede, este será o seu primeiro alvo de ataque. Para isso, devem ser estudadas todas as possibilidades para a sua escolha, instalação e configuração.

3.2.7 Cifra

A cifra é um algoritmo utilizado para a encriptação de dados, permitindo codificá-los, tornando-os assim inacessíveis para a maioria das pessoas, e legíveis apenas para as pessoas que conheçam a chave[27]. A certificação digital (que se verá mais à frente) serve-se da tecnologia de criptografia assimétrica.

3.2.8 Wireless específico

A utilização de wireless específico torna mais segura a transferência de informação entre computadores pertencentes à mesma rede.

3.2.9 Biometria informática

No combate à fuga da informação, é muito importante conseguir identificações fiáveis dos colaboradores das organizações ou das pessoas que têm acesso a determinados tipos de serviços. Para isso existem já tecnologias de informação muito desenvolvidas, uma delas é a chamada biometria informática. Esta técnica de reconhecimento consiste num sistema electrónico que permite reconhecer as pessoas através de características (físicas ou não)[28].
Exemplos dessas características são: voz, mãos, face, íris[29], veias, assinatura, …, digitação.
Das enumeradas, as mais fiáveis são a face, as veias e a íris.

---

[27] *In* "Kimaldi: Àrea de Conhecimento Assinatura Digital." from http://www.sankhya.com.br/glossario_a.php.

[28] *In* "Colégio Web." Retrieved 2010, from http://www.colegioweb.com.br/curiosidades/biometria.html.

[29] **íris** é a parte mais visível (e colorida) do olho

4 Certificação digital[30] (Definição e utilidade)

4.1 O que é a certificação digital e para que serve?

A certificação digital, funcionando à base de uma chave pública denominada de PKI (Public Key Infrastructure), é, como o próprio nome indica, uma plataforma utilizada para garantir a segurança nos documentos electrónicos. Normalmente a certificação digital assegura aos seus clientes os critérios básicos para a segurança da informação: Integridade; Identificação; Confidencialidade; Aceitação. Com a confidencialidade garante-se que a informação não é violada;

Para garantir um processo eficaz de **Autenticação/Identificação**, é atribuído uma espécie de código digital a cada parte envolvida. Esse código permitirá provar a identidade dos envolvidos de uma forma segura. No que consiste à Integridade da informação, um bom certificado digital deve permitir a detecção de eventuais alterações da informação por parte de terceiros. Quanto ao reconhecimento da origem, através de um certificado digital deverá ser possível determinar a autenticidade da origem da mensagem. Quanto à aceitação das mensagens, deve ser possível rejeitar automaticamente as mensagens fraudulentas e aceitar as mensagens autênticas.

De uma forma geral, a certificação digital é utilizada para transmitir documentos electrónicos através de uma rede, tendo a garantia de que são cumpridos todos os critérios de segurança.

4.2 PKI: como funciona?

São atribuídos dois códigos/chaves a cada utilizador: uma chave privada e uma chave pública. Essas duas chaves estão associadas entre si através de uma função matemática, não sendo possível a obtenção de uma chave pública através de uma chave privada, ou vice-versa. Enquanto a chave pública é disponibilizada a todos, apenas o próprio utilizador conhece a sua chave privada. Os dados codificados na chave pública estão descodificados na chave privada e vice-versa.

4.2.1 Como tudo se processa

Através de uma sequência de bytes o ficheiro é emitido e assinado digitalmente pela entidade de certificação, estabelecendo uma ligação à chave pública, de modo a que a identidade do emissor seja clara para o receptor da mensagem. Para definir o necessário período de validação da mensagem, é necessário utilizar um carimbo de tempo, ou *timestamp*, que é emitido por uma terceira entidade.

[30] *In* Multicert. "Certificados digitais." 2010, from https://www.multicert.com/certificadosdigitais.

Um *timestamping* é idêntico a uma assinatura electrónica, contendo a data/hora, fornecida por uma fonte de tempo legal. A sua utilidade é a de que permite detectar alterações ao documento feitas após a introdução do carimbo.

A assinatura digitalizada permite a terceiras entidades alterar o documento sem que ninguém se aperceba.

4.3 Certificado digital qualificado

O artº 3º do Decreto de Lei 62/2003 postula que: quando dotado de uma assinatura electrónica certificada, o documento electrónico tem o mesmo valor legal que um documento particular assinado;

O artº5º do mesmo Decreto de Lei, estabelece que: é possível aos órgãos públicos emitir documentos electrónicos com a assinatura qualificada, desde que esta respeite as normas constantes na presente lei. No que respeita à criação, emissão, reprodução, arquivo, transmissão e cópia de documentos electrónicos relativos a actos administrativos (tudo isso feito informaticamente), deve proceder-se à clarificação dos respectivos actos, tornando mais fácil identificá-los, e deve também ser comprovada a função desempenhada pela pessoa que assina cada documento.

Ainda neste mesmo Decreto de Lei, o artº7º determina o que um documento electrónico dotado com uma assinatura electrónica certificada tem o mesmo valor que um documento em papel autenticado com uma assinatura manual. Presumindo-se pois que o individuo que colocou a assinatura electrónica é o seu legitimo titular, e subentende-se logicamente que essa assinatura foi colocada com o objectivo de legitimar o documento electrónico. Depreende-se também que a partir do momento em que foi assinado o documento electrónico não foi alterado.

O Decreto de Lei 62/2003, não é a única disposição legal relativamente aos certificados digitais, um outro artigo que se destaca é o artigo 376.o do Código Civil, que estipula que: no caso de um documento electrónico cujo conteúdo não seja susceptível de ser representado através de um documento escrito, este tem o valor legal de acordo com o previsto no artigo 368.o do Código Civil e no artigo 167.o do Código de Processo Penal.

4.4 Como obter um certificado digital?

Podem ser obtidos variados tipos de certificados digitais: certificado digital para pessoa singular, certificado digital para pessoa singular profissional ou certificado digital para pessoa colectiva.

Todavia, o processo de obtenção do certificado digital é similar em todos os casos: consulta-se a documentação exigida pela entidade autorizada a emitir esse tipo de certificados e ao preenchimento do formulário disponibilizado, após o que se procede ao envio da documentação e do formulário para a respectiva entidade.

5 Três categorias de aplicações de segurança…

Em jeito de conclusão no que respeita às tecnologias de informação, pode dizer-se que existem três diferentes tipos de aplicações que trabalham para garantir a segurança da informação[31]. São elas:

1. Aplicações de segurança de rede;
2. Aplicações de software;
3. Aplicações de segurança de dados.

As aplicações de segurança de rede são um misto de aplicações que garantem uma maior segurança de rede, segurança de dados e protecção de software. Ao abrangerem ataques externos contra fontes de informação protegidas pelos programas de firewall proporcionam uma protecção de rede. As aplicações de segurança de rede protegem e garantem a disponibilidade dos serviços de rede e normalmente servem-se de programas de firewall, sistemas de detecção de intrusos, sistemas de prevenção contra intrusões, autenticação e programas antivírus.
Por sua vez, as aplicações de software têm a função de, como o próprio nome indica, proteger o software e os dados que este contém, contra os diversos tipos de ataques.

Quanto às aplicações de segurança de dados, destina-se a proteger os dados utilizados e armazenados localmente ou transmitidos entre os utilizadores através de uma rede, sendo o tipo de protecção mais utilizada a protecção criptográfica.

É importante referir que as aplicações de segurança vão sofrendo uma evolução proporcional ao aumento da complexidade dos ataques, no entanto, estão sempre a surgir novos tipos de ataques e as aplicações actuais muitas vezes já não estão à altura desses ataques, pelo que é necessário estar sempre na vanguarda.

6 Normalização da informação

6.1 Norma ISO 17799

Esta norma está organizada/estruturada nos seus pontos essenciais da forma apresentada imediatamente a seguir:

6.1.1 Política de segurança

O Objectivo da Política de Segurança da Informação é de dar apoio à gestão para a segurança da informação.

[31] In Main, A. (2004). "Application Security: Building in Security during the Development Stage." Information Security Journal **13**(2): 7.

A gestão deve estabelecer uma direcção política clara e demonstrar suporte, e compromisso com, a segurança da informação através da emissão e manutenção de uma política de segurança da informação para toda a organização.

Um documento com a política de segurança da informação deve ser aprovado, publicado e divulgado, conforme apropriado, para todos os empregados. Ele deve declarar o compromisso da gestão e estabelecer a abordagem da organização quanto à gestão da segurança da informação.

A política deve ter um responsável pela manutenção e revisão de acordo com um processo de revisão definido. Esse processo deve assegurar que seja executada uma revisão em resposta a quaisquer mudanças que afectem a base da avaliação de risco original, por exemplo episódios de segurança significativos, novas vulnerabilidades ou mudanças na infra-estrutura organizacional ou técnica. Também devem ser programadas revisões periódicas de aspectos como: a eficácia da política, demonstrada pela natureza, quantidade e impacto dos incidentes de segurança comedidos; o custo e impacto dos controlos na eficiência do negócio e os efeitos das mudanças na tecnologia.

6.1.2 Segurança organizacional

Infra-estrutura para Segurança da Informação

O objectivo da Infra-estrutura para Segurança da Informação é de gerir a segurança da informação dentro da organização.

Segurança da Informação é uma responsabilidade corporativa compartilhada por todos os membros da equipa de gestão. Portanto, deve ser considerado um fórum de gestão para assegurar a existência de direcção clara e suporte visível por parte da gestão para as iniciativas de segurança. Esse fórum deve promover a segurança dentro da organização através de compromisso apropriado e alocação de recursos adequados. Geralmente, tal fórum encarrega-se do seguinte: rever e aprovar a política de segurança da informação e responsabilidades gerais; monitorizar mudanças significativas na exposição dos bens de informação às principais ameaças; rever e monitorizar incidentes que afectem a segurança da informação e aprovar as iniciativas importantes para aprimorar a segurança da informação.

Um gestor deve ser responsável por todas as actividades relacionadas com a segurança.

Numa organização de grande porte, pode ser necessário um fórum inter-funcional de representantes da gestão de sectores relevantes da organização para coordenar a implementação de controlos de segurança da informação. Geralmente, um fórum desse tipo: concorda sobre papéis e responsabilidades específicos para segurança da informação em toda a organização; concorda sobre metodologias e processos específicos para segurança da informação, por exemplo avaliação de riscos e sistema de classificação de segurança; concorda e apoia

iniciativas de segurança da informação que abrangem toda a organização; por exemplo, programas de consciencialização sobre segurança; assegura que a segurança seja parte do processo de planeamento de informação; avalia a adequação e coordena a implementação de controlos específicos para segurança da informação em novos sistemas ou serviços; fiscaliza os incidentes relacionados com a segurança da informação e fomenta a visibilidade do suporte corporativo para a segurança da informação em toda a organização.

As responsabilidades pela protecção de bens individuais e pela condução de processos de segurança específicos devem ser claramente definidas.

A política de segurança da informação deve proporcionar uma orientação geral sobre a alocação de papéis e responsabilidades relacionados à segurança na organização. Isto deve ser implementado, onde fôr necessário, com orientação mais detalhada para *sites*, sistemas ou serviços específicos.

Em muitas organizações, um gestor de segurança da informação será designado para assumir a responsabilidade geral pelo desenvolvimento e implementação da segurança e para dar suporte à identificação dos controlos.

Entretanto, a responsabilidade pela alocação de recursos e implementação dos controlos frequentemente permanecerá com gestores individuais.

É essencial que as áreas pelas quais cada gestor é responsável sejam claramente definidas e em especial, deve coincidir o seguinte: os vários bens e processos de segurança associados com cada sistema individual devem ser identificados e claramente definidos; deve haver concordância quanto ao gestor responsável por cada activo ou processo de segurança e os detalhes dessa responsabilidade devem ser documentados bem como os níveis de autorização que também devem ser claramente definidos.

Um processo de gestão de autorização para novas facilidades de processamento de informação deve ser implantado consideradando novas facilidades e com a devida aprovação, autorizando os seus propósitos e uso. Também deve ser obtida a aprovação do gestor responsável pela manutenção do ambiente local de segurança de sistemas de informação para assegurar que são atendidas todas as políticas e exigências relevantes; se for necessário, o hardware e o software devem ser verificados para assegurar que eles são compatíveis com outros componentes do sistema, o uso de facilidades pessoais de processamento de informação para processar informação do negócio e quaisquer controlos necessários têm que ser autorizados, uma vez que o uso de facilidades pessoais de processamento de informação no local de trabalho pode acarretar novas vulnerabilidades, (o que justifica a sua necessidade de avaliação e autorização).

Estes controlos são especialmente importantes em ambientes que utilizam redes. É muito provável que seja necessário, em muitas organizações, um aconselhamento especializado

sobre segurança da informação. Idealmente, um consultor interno experiente em segurança de informação deve ter a capacidade de desempenhar essa função.

Os consultores de segurança da informação, devem ter como tarefa fornecer um aconselhamento sobre todos os aspectos da segurança da informação. A qualidade das suas avaliações sobre as ameaças à segurança e de seu aconselhamento sobre os controlos determinarão a efectividade da segurança de informação na organização.

O consultor de segurança de informação, deve ser consultado o mais cedo possível a partir do momento em que há suspeita de um incidente ou quebra de segurança, para que possa actuar como uma fonte de orientação especializada ou recursos de investigação.

Os contactos apropriados com autoridades policiais, órgãos regulamentadores, provedores de serviços de informação e operadoras de telecomunicações devem ser mantidos para garantir que a acção apropriada seja tomada rapidamente, e obtido aconselhamento, na eventualidade de um incidente de segurança.

O intercâmbio de informação de segurança deve ser restrito para assegurar que as informações confidenciais da organização não sejam encaminhadas para pessoas não autorizadas.

O documento sobre a política de segurança da informação estabelece a política e as responsabilidades pela segurança da informação.

Segurança para o acesso de terceiros

O objectivo da Segurança para o acesso de terceiros é de manter a segurança nas facilidades de processamento de informação organizacionais e bens de informação consultados por terceiros. O acesso por terceiros às facilidades de processamento de informação da organização deve ser controlado.

Quando houver uma necessidade de fornecer acesso a terceiros para garantir a concretização de um negócio, deverá em primeiro lugar efectuada uma avaliação de riscos para determinar as implicações de segurança e as exigências. Os controlos devem ser acordados e definidos através de um contrato com a terceira parte.

Outsourcing

O objectivo do Outsourcing é o de manter a segurança da informação quando a responsabilidade pelo processamento da informação tiver sido “terceirizada” com outra organização.

Os acordos de outsourcing devem tratar dos riscos, controlos de segurança e procedimentos para os sistemas de informação, ambientes de rede e/ou desktop no contrato entre as partes.

Os requisitos de segurança de uma organização que “terceiriza” a gestão e o controlo de todos ou alguns dos sistemas de informação, ambientes de redes e/ou ambientes de desktop

devem ser tratados num contrato acordado entre as partes que deve mencionar: como exigências legais a serem satisfeitas.

6.1.3 Classificação e controlo dos bens

Responsabilidade pelos bens

O objectivo é de manter uma protecção apropriada para os bens organizacionais.

Todos os bens de informação mais importantes devem ter um proprietário nominal, responsável por eles.

A responsabilidade pelos bens ajuda a assegurar que seja mantida uma protecção adequada. Os proprietários devem ser identificados para todos os bens importantes e a responsabilidade pela manutenção dos controlos apropriados deve ser atribuída. A responsabilidade pela implementação dos controlos pode ser delegada. A responsabilidade final deve permanecer com o proprietário do bem.

Um inventário dos bens ajuda a assegurar que ocorra uma protecção efectiva dos bens, e também pode ser exigido para outros fins do negócio, tais como razões de higiene e segurança, seguros ou motivos financeiros. O processo de compilar um inventário de bens é um aspecto importante da administração de riscos. Uma organização deve ser capaz de identificar os seus bens, bem como a importância e o valor relativos desses bens. Baseada nessas informações, uma organização pode então prover níveis de protecção proporcionais ao valor e importância dos bens.

Classificação da informação

O objectivo é garantir que os bens de informação recebam um nível de protecção adequado. As informações devem ser classificadas para indicar a necessidade, as prioridades e o grau de protecção. As informações apresentam graus variáveis de susceptibilidade e de crítica. Alguns itens podem exigir um nível adicional de protecção ou tratamento especial. Um sistema de classificação da informação deve ser usado para definir um conjunto apropriado de níveis de protecção e comunicar a necessidade de medidas de tratamentos especiais.

As classificações e controlos de protecção para as informações devem considerar as necessidades do negócio quanto à partilha ou restrição das informações, e os impactos para o negócio associados a tais necessidades.

As informações e as saídas geradas pelos sistemas que tratam dados confidenciais devem ser rotuladas segundo o seu valor e sensibilidade para a organização. Também pode ser apropriado rotular informação em termos da importância que esta tem para a organização. As informações deixam frequentemente de ser sensíveis ou críticas após um certo período de

tempo. Esses aspectos devem ser levados em conta, assim como também o facto de uma classificação excessiva poder levar a despesas adicionais desnecessárias. As directrizes para a classificação devem prever e admitir o facto de que a classificação de um item qualquer de informação não é necessariamente fixa ao longo do tempo, e pode mudar de acordo com alguma política predeterminada.

Deve-se levar em consideração a quantidade de categorias de classificação e os benefícios a serem obtidos com o seu uso. É importante que um conjunto apropriado de procedimentos seja definido para a rotulagem das informações de acordo com o esquema de classificação adoptado pela organização. Esses procedimentos têm de cobrir os bens de informação nos formatos físicos e electrónicos.

6.1.4 Segurança relacionada com o pessoal

Segurança na definição de funções e alocação de pessoal

O objectivo é de reduzir os riscos de erros humanos, roubos ou uso indevido das facilidades.

As responsabilidades de segurança devem ser tratadas no estágio de recrutamento, incluídas em contratos durante o tempo que o indivíduo estiver no emprego.

Os candidatos potenciais devem ser adequadamente seleccionados, especialmente para as funções sensíveis. Todos os empregados e utilizadores "terceirizados" das facilidades de processamento de informação devem assinar um contrato de confidencialidade (não divulgação).

Os papéis de segurança e as responsabilidades, conforme delineados na política de segurança de informação da organização, devem incluir as responsabilidades gerais pela implementação ou manutenção da política de segurança bem como todas as responsabilidades específicas pela protecção de determinados bens, ou pela execução de determinados processos ou actividades de segurança.

Para os empregados permanentes, no momento das propostas de emprego, devem ser efectuadas verificações de confirmação.

Quando na contratação inicial ou na promoção, se envolver uma pessoa com acesso às facilidades de processamento de informação, e em particular se esta lidar com informação sensível, a organização também deve executar uma verificação de crédito.

Contratos de confidencialidade ou não divulgação são utilizados para avisar que informações são confidenciais ou secretas. Os empregados devem normalmente assinar tal contrato como parte integrante dos termos e condições iniciais de emprego.

Nos termos e condições de emprego devem constar a responsabilidade do empregado pela segurança da informação. As responsabilidades e direitos legais do empregado, por

exemplo, com respeito a leis de *copyright* ou legislação de protecção de dados, devem ser esclarecidas e incluídas nos termos e condições do contrato de trabalho.

Formação dos utilizadores

O objectivo é assegurar que os utilizadores se consciencializem das preocupações e ameaças à segurança da informação, e estejam preparados para apoiar a política de segurança organizacional no curso do seu trabalho normal. Os utilizadores devem ser treinados nos procedimentos de segurança e no uso correcto das facilidades de processamento de informação para minimizar os possíveis riscos de segurança.

Respondendo a incidentes de segurança e mau funcionamento

O objectivo é de minimizar os danos resultantes de incidentes de segurança e mau funcionamento, e monitorizar e aprender com tais incidentes, que afectam a segurança e que devem ser reportados através de canais administrativos apropriados o mais rapidamente possível.

Todos os empregados e contratados devem estar cientes dos procedimentos para reportar os diferentes tipos de incidente que possam ter impacto na segurança dos bens organizacionais.

Os incidentes de segurança devem ser reportados através dos canais administrativos adequados o mais rapidamente possível.

Todos os empregados e contratados devem estar cientes do procedimento para reportar incidentes de segurança, e deve-se exigir que reportem tais incidentes o mais rápido possível. Processos de *feedback* adequados devem ser implementados para garantir que aqueles que reportaram os incidentes sejam notificados dos resultados após o incidente ser investigado e encerrado.

Os utilizadores de serviços de informação devem ser obrigados a anotar e reportar quaisquer pontos fracos observados, ou ameaças, nos sistemas e serviços.

Os utilizadores devem ser informados de que eles não devem, em nenhuma circunstância, tentar provar (testar) um ponto fraco suposto.

Devem ser estabelecidos procedimentos para reportar mau funcionamento de softwares. Os utilizadores não devem tentar remover o software suspeito a menos que sejam autorizados a fazê-lo. A recuperação deve ser executada por pessoal adequadamente treinado e experiente; devem existir mecanismos para capacitar a quantificação dos tipos, volumes e custos dos incidentes e maus funcionamentos. Essas informações devem ser usadas para identificar incidentes ou maus funcionamentos recorrentes ou de alto impacto. E devem existir um processo disciplinar formal para empregados que tenham violado as políticas e procedimentos de segurança organizacionais.

6.1.5 Segurança física e ambiental

Áreas de segurança

O Objectivo é de impedir o acesso não autorizado, danos ou interferência às instalações físicas e às informações da organização.

As facilidades de processamento de informação sensíveis ou críticas para o negócio devem ser localizadas em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controlos de entrada. Elas devem ser fisicamente protegidas contra acesso não autorizado, danos e interferências.

A protecção física pode ser obtida criando-se diversas barreiras físicas em torno dos edifícios e das facilidades de processamento de informação da organização. Cada barreira estabelece um perímetro de segurança, cada um aumentando a protecção total fornecida. As organizações devem usar perímetros de segurança para proteger áreas que contenham facilidades de processamento de informação.

Segurança dos equipamentos

O Objectivo é impedir perda, danos ou compromisso de bens e interrupção das actividades do negócio.

Os equipamentos devem ser fisicamente protegidos contra ameaças à segurança e perigos ambientais. A protecção dos equipamentos é necessária para reduzir o risco de acesso não autorizado aos dados e para os proteger contra perda ou danos. Deve-se também considerar a localização dos equipamentos e a sua disposição física.

Os equipamentos devem ser protegidos, ou dispostos fisicamente de forma adequada, para reduzir os riscos oriundos de ameaças e perigos ambientais e de oportunidades de acesso não autorizado.

Os equipamentos devem ser protegidos contra a falta de energia e outras anomalias na electricidade. Uma fonte eléctrica adequada deve ser provida de acordo com as especificações do fabricante do equipamento.

Um equipamento de "***no-break***" para suportar um encerramento do processamento de forma ordenada ou para continuar com o processamento é recomendado para equipamentos que suportam operações críticas para o negócio. Os planos de contingência devem cobrir a acção a ser executada no caso de falha do "***no-break***". O equipamento de "***no-break***" deve ser verificado regularmente, para certificar que ele possui a capacidade adequada, e deve ser testado de acordo com as recomendações do fabricante.

Os cabos de energia e telecomunicação que transportam dados ou suportam serviços de informação devem ser protegidos contra interceptação ou danos.

Os equipamentos devem ser correctamente conservados para assegurar a sua disponibilidade e integridade continuadas.

Independentemente da propriedade, o uso de qualquer equipamento fora das instalações físicas da organização para processamento de informação deve ser autorizado pela gerência. A segurança fornecida deve ser equivalente àquela dos equipamentos ***on-site*** usados para o mesmo propósito, levando-se em consideração os riscos de trabalhar fora do local da organização.

As informações podem ser comprometidas através da exclusão ou reutilização descuidada dos equipamentos. Os dispositivos de armazenamento que tenham informação sensíveis devem ser fisicamente destruídos ou regravados de forma segura em vez de se usar a função padrão "***delete***".

Controlos gerais

O objectivo é de impedir o compromisso ou roubo de informação e de facilidades de processamento de informação.

As informações e as facilidades de processamento de informação devem ser protegidas contra a divulgação, modificação ou roubo por pessoas não autorizadas, e devem ser implementados controlos para minimizar perdas ou danos.

Os equipamentos, informação ou software não devem ser retirados das instalações da organização sem autorização. Quando necessário e apropriado, deve proceder-se ao registo da saída dos equipamentos, tal como do seu retorno.

6.1.6 Gestão de Comunicações e operações

Procedimentos operacionais e responsabilidades

O objectivo é garantir a operação correcta e segura das facilidades de processamento de informação.

As responsabilidades e os procedimentos para a gestão e operação de todas as facilidades de processamento de informação devem ser estabelecidos. Isso inclui o desenvolvimento de instruções de operação apropriadas e de procedimentos para resposta a incidentes.

Os procedimentos operacionais identificados pela política de segurança devem ser documentados e mantidos actualizados, devendo também ser tratados como documentos formais e as alterações devem ser autorizadas pela gerência.

As mudanças nas facilidades de processamento de informação e nos sistemas devem ser controladas. O controlo inadequado dessas mudanças é uma causa frequente de falhas na segurança ou nos sistemas.

Os programas operacionais devem estar sujeitos a um controlo restrito das alterações. Quando os programas são alterados, deve ser retido um "***log***" para auditoria, contendo todas as informações relevantes.

Alterações no ambiente operacional podem causar impacto nos aplicativos. Onde for praticável, os procedimentos para controlo das mudanças operacionais e nos aplicativos deve ser integrado.

A segregação de tarefas é um método de reduzir o risco de má utilização acidental ou deliberada do sistema. Deve-se considerar a separação da gestão ou da execução de determinadas tarefas ou áreas de responsabilidade, para reduzir as oportunidades de modificação não autorizada ou utilização indevida das informações ou serviços.

Separar as facilidades de desenvolvimento, testes e produção é importante para se obter a segregação dos papéis envolvidos. As regras para transferência de software do desenvolvimento para o status operacional devem ser definidas e documentadas.

As actividades de desenvolvimento e testes podem causar sérios problemas, tais como a modificação indesejada de arquivos ou do ambiente de desenvolvimento, ou falha no sistema. Deve ser considerado o nível de separação que é necessário, entre ambientes de produção, testes e desenvolvimento, para impedir problemas operacionais. Uma medida semelhante também deve ser implementada entre as funções de desenvolvimento e teste. Neste caso, existe uma necessidade de se manter um ambiente estável e conhecido, no qual se possa executar testes significativos, e de impedir o acesso inadequado pelo investigador.

Onde as equipas de desenvolvimento e testes tiverem acesso ao sistema operacional e às suas informações, eles podem ser capazes de introduzir código não autorizado e não testado ou alterar dados operacionais. Nalguns sistemas, essa capacidade pode ser usada impropriamente para cometer fraudes ou introduzir código malicioso ou não testado.

As actividades de desenvolvimento e de testes podem causar alterações não intencionadas ao software e às informações se elas compartilharem o mesmo ambiente computacional.

A utilização de uma empresa externa contratada para gerir as facilidades de processamento de informação pode introduzir uma exposição potencial de segurança, tal como a possibilidade de compromissos, danos ou perdas de dados no *site* da empresa contratada.

Planeamento e aceitação de sistemas

O objectivo é minimizar os riscos de falhas nos sistemas.

O planeamento antecipado e preparação são obrigatórios para assegurar a disponibilidade das capacidades e recursos adequados. Devem ser feitas projecções das necessidades futuras de capacidade, para reduzir o risco de sobrecarga no sistema.

Os critérios de aceitação para novos sistemas de informação, *upgrades* e novas versões devem ser estabelecidos e devem ser realizados testes adequados aos sistemas antes da aceitação. Os gerentes devem garantir que os requisitos e os critérios para aceitação de novos sistemas estão claramente definidos, concordados, documentados e testados.

Para novos desenvolvimentos importantes, a área de produção e os utilizadores devem ser consultados em todos os estágios do processo de desenvolvimento para garantir a eficiência operacional do projecto do sistema proposto. Testes apropriados devem ser conduzidos para confirmar que todos os critérios de aceitação estão plenamente satisfeitos.

Protecção contra software malicioso

O objectivo é proteger a integridade de softwares e informação. Essas precauções são necessárias para impedir e detectar a introdução de softwares maliciosos. Os utilizadores devem ser consciencializados dos perigos relacionados com software malicioso ou não autorizado, e os gestores devem, quando necessário, implementar controlos especiais para detectar ou impedir a sua introdução.

Devem ser implementados controlos para detecção e prevenção contra softwares maliciosos e procedimentos apropriados para consciencializar os utilizadores. A protecção contra software malicioso deve ser baseada na consciencialização sobre segurança, acesso apropriado ao sistema e controlos para gestão de alterações.

Housekeeping

O objectivo é manter a integridade e a disponibilidade dos serviços de processamento de informação e comunicações. Devem ser executadas regularmente cópias ***backup*** dos softwares e das informações essenciais para o negócio.

Gestão de redes

O objectivo é assegurar a salvaguarda de informação em redes de computadores e a protecção da infra-estrutura de apoio. A gestão da segurança em redes - que pode ultrapassar as fronteiras da organização - exige atenção.

Diversos controlos são necessários para obter e manter a segurança em redes de computadores.

Os gestores de redes devem implementar controlos para garantir a segurança dos dados nas redes e a protecção de serviços que se utilizam nas redes contra acesso não autorizado.

Intercâmbios de informação e softwares

O objectivo é impedir perda, modificação ou uso indevido de informação intercambiadas entre organizações.

Os intercâmbios de informação e software entre organizações deve ser controlado e deve obedecer a qualquer legislação relevante. Os intercâmbios devem ser executados com base em contratos.

As informações podem ser vulneráveis a acesso não autorizado ou uso indevido durante transporte físico.

O comércio electrónico pode envolver o uso de intercâmbio de dados electrónicos (EDI), correio electrónico e transacções *online* através de redes públicas, como a

Internet. O comércio electrónico é vulnerável a muitas ameaças pela rede, que podem resultar numa actividade fraudulenta, disputa contratual e divulgação ou modificação de informação.

O correio electrónico vem sendo usado para comunicações comerciais, substituindo as formas tradicionais. O correio electrónico difere das formas tradicionais de comunicação comercial, por exemplo, pela sua velocidade, estrutura de mensagens, grau de informalidade e vulnerabilidade a acções não autorizadas.

As políticas e directrizes devem ser preparadas e implementadas para controlar os riscos para a segurança e para o negócio associados com sistemas de automação de escritórios. Estes propiciam oportunidades para disseminação e partilha mais rápida de informação comercial usando uma combinação de: documentos, computadores, computação móvel, comunicações móveis, correio, correio de voz, comunicações verbais em geral, multimédia, serviços/facilidades postais e equipamentos de fax.

Devem ser tomadas medidas para proteger a integridade de informação publicada electronicamente para impedir a modificação não autorizada, que poderia prejudicar a reputação da organização que publica. As informações de um sistema disponibilizado publicamente, tal como informação num servidor de Web acessíveis via Internet, podem necessitar de obedecer a leis, normas e regulamentos na jurisdição onde o sistema está localizado ou onde os negócios ocorrem.

6.1.7 Necessidades de controlo de acesso

O objectivo é controlar o acesso às informações

O acesso a informação e processos do negócio deve ser controlado com base nas necessidades de segurança e do negócio e devem ser tidas em conta as políticas para disseminação e autorização das informações. Os requisitos de controlo de acesso na organização devem ser definidos e documentados. As regras e direitos de controlo de acesso para cada utilizador ou grupo de utilizadores devem ser claramente definidas numa declaração de política de acesso.

Os utilizadores e os provedores de serviços devem receber uma declaração clara dos requisitos a serem satisfeitos pelos controlos de acesso.

Gestão do acesso de utilizadores

O objectivo é de impedir acesso não autorizado aos sistemas de informação.

Os procedimentos formais devem ser implementados para controlar a alocação de direitos de acesso a sistemas e serviços de informação.

Os procedimentos devem cobrir todos os estágios do ciclo de vida do acesso dos utilizadores, desde o registo inicial de novos utilizadores até a retirada final do mesmo, que não necessita mais de ter acesso aos sistemas e serviços de informação.

O acesso a serviços de informação multiutilizadores deve ser controlado através de um processo formal de registo de utilizadores.

A alocação e o uso de privilégios devem ser restritos e controlados. O uso inapropriado de privilégios de um sistema é um dos principais factores contribuintes para a falha de sistemas que foram violados.

As senhas são um meio comum de validar a identidade de um utilizador para consultar um sistema ou serviço de informação.

Responsabilidades dos utilizadores

O objectivo é impedir o acesso de utilizadores não autorizados.

A cooperação dos utilizadores autorizados é essencial para a eficácia da segurança.

Os utilizadores devem ser consciencializados de suas responsabilidades quanto à manutenção de controlos eficazes de acesso, particularmente o uso de senhas e à segurança do equipamento do utilizador.

Os utilizadores devem assegurar-se de que os equipamentos não assistidos possuem protecção apropriada. Os equipamentos instalados nas áreas dos utilizadores, como estações de trabalho ou servidores de arquivos, podem exigir protecção específica contra acesso não autorizado quando deixados sem assistência por um período prolongado. Todos os utilizadores e contratados devem ser consciencializados dos requisitos e procedimentos de segurança para proteger o equipamento não assistido, bem como das suas responsabilidades para a implementação de tal protecção.

Controlo de acesso à rede

O objectivo é a protecção dos serviços que utilizam redes.

O acesso a serviços em redes internas e externas deve ser controlado. Isto é necessário para assegurar que os utilizadores que têm acesso a redes e serviços em rede não comprometam a segurança de tais serviços. Relações inseguras com serviços numa rede podem afectar toda a organização. Os utilizadores devem ter acesso directo apenas aos serviços aos quais foram especificamente autorizados a usar. Este controlo é particularmente importante para ligações de rede com aplicações sensíveis ou críticas ou para utilizadores em locais de alto risco, como áreas públicas ou externas que estão fora da gestão e controlo de segurança da organização.

Ligações externas apresentam um potencial para acesso não autorizado às informações do negócio, como por exemplo acesso através de métodos ***dial-up***. O acesso de utilizadores remotos deve estar sujeito à autenticação. Existem tipos diferentes de métodos de autenticação e alguns fornecem um nível de protecção maior do que outros, tais como métodos baseados no uso de técnicas criptográficas, que podem proporcionar uma autenticação mais poderosa. É importante determinar o nível de protecção requerida a partir de uma avaliação de riscos. Isto é necessário para a selecção apropriada de um método de autenticação. A autenticação de utilizadores remotos pode ser conseguida usando-se, por exemplo, uma técnica baseada em

criptografia, ***tokens*** de hardware ou protocolo tipo "***challenge/response***". Linhas privadas dedicadas ou uma funcionalidade para verificar endereços de utilizador na rede também podem ser usadas para fornecer garantia da origem das ligações. Um recurso para ligação automática com um computador remoto pode fornecer um meio para obter acesso não autorizado a uma aplicação da organização. Ligações com sistemas de computadores remotos devem portanto ser autenticadas. Isto é especialmente importante se a ligação usar uma rede que está fora do controlo da gestão de segurança da organização.

O acesso a portas de diagnóstico deve ser controlado de forma segura. Muitos computadores e sistemas de comunicação são instalados como um recurso de diagnóstico remoto. Se desprotegidas, estas portas de diagnóstico propiciam um meio para acesso não autorizado. Portanto, elas devem ser protegidas por um mecanismo de segurança adequado, como um ***key lock***, e um procedimento para garantir que elas sejam acessíveis apenas através de combinação entre o gestor do serviço de computador e o pessoal de suporte de hardware/software que solicitar o acesso.

As redes estão cada vez mais a estender-se além das fronteiras tradicionais das organizações, à medida que são formadas parcerias comerciais que podem necessitar de interligação ou partilha de facilidades de processamento de informação e redes. Tais extensões podem aumentar o risco de acesso não autorizado aos sistemas de informação que já usam a rede, alguns dos quais podem exigir protecção contra outros utilizadores da rede devido à sua confidencialidade. Em tais circunstâncias, a introdução de controlos dentro da rede, para segregar grupos de serviços de informação, utilizadores e sistemas de informação, deve ser considerada.

Os requisitos da política de controlo de acesso para redes compartilhadas, especialmente aquelas que se estendem além das fronteiras da organização, podem exigir a incorporação de controlos para restringir a capacidade de ligação dos utilizadores.

As redes compartilhadas, especialmente aquelas que cruzam as fronteiras da organização, podem exigir a incorporação de controlos para assegurar que as ligações entre computadores e os fluxos de informação não violem a política de controlo de acesso das aplicações do negócio.

Está disponível uma vasta gama de serviços de redes públicas ou privadas, algumas das quais oferecem serviços com valor agregado. Os serviços de rede podem ter características de segurança únicas ou complexas. As organizações que usam serviços de rede devem assegurar-se que é fornecida uma descrição clara dos atributos de segurança de todos os serviços usados.

O Controlo de Acesso às Aplicações

O objectivo é impedir acesso não autorizado às informações mantidas nos sistemas de informação. Os recursos de segurança devem ser usados para restringir o acesso dentro dos sistemas aplicativos.

Os utilizadores de sistemas aplicativos, incluindo a equipa de suporte, devem receber acesso às informações e funções dos sistemas aplicativos de acordo com uma política predefinida de controlo de acesso, baseada nos requisitos individuais das aplicações do negócio e consistente com a política organizacional de acesso a informação.
Os sistemas sensíveis podem exigir um ambiente computacional dedicado (isolado).

Alguns sistemas aplicativos são suficientemente sensíveis a perdas potenciais a ponto de exigir tratamento especial. A sensibilidade pode indicar que o sistema aplicativo deve ser executado num computador dedicado, deve compartilhar recursos apenas com sistemas aplicativos confiáveis ou não ter limitações.

6.1.8 Desenvolvimento e manutenção de sistemas

Requisitos de segurança nos sistemas

O objectivo é assegurar que a segurança seja encaixada nos sistemas de informação. Isto incluirá infra-estrutura, aplicações do negócio e aplicações desenvolvidas pelos utilizadores. O projecto e a implementação do processo corporativo que dá suporte à aplicação ou ao serviço pode ser crucial para a segurança. Os requisitos de segurança devem ser identificados e acordados antes do desenvolvimento de sistemas de informação.

Os relatórios relativos aos requisitos do negócio para novos sistemas, ou melhorias em sistemas existentes, devem especificar as necessidades de controlos. Tais especificações devem considerar os controlos automatizados a serem incorporados no sistema e a necessidade de suportar controlos manuais.

Os requisitos de segurança e controlos devem reflectir o valor para o negócio dos bens de informação envolvidos e o prejuízo potencial para o negócio, que poderia resultar de uma falha ou ausência de segurança. A base para se analisar os requisitos de segurança e identificar os controlos para satisfazê-los é a avaliação de riscos e gestão de riscos.

Segurança em sistemas aplicativos

O objectivo é impedir perda, modificação ou má utilização de dados dos utilizadores em sistemas aplicativos. Controlos apropriados e ***audit trails*** ou ***logs*** de actividades devem ser projectados nos sistemas aplicativos, incluindo aplicativos escritos pelos utilizadores.
A entrada de dados para os sistemas aplicativos deve ser validada para garantir que está correcta e apropriada. E, devem ser efectuadas verificações à entrada de transacções comerciais, dados de registo e tabelas de parâmetros.

Dados que foram correctamente introduzidos podem ser corrompidos por erros de processamento ou através de actos deliberados. O projecto das aplicações deve assegurar que sejam implementadas restrições para minimizar o risco de falhas de processamento que levem a

uma perda de integridade. Os controlos exigidos dependerão da natureza do aplicativo e do impacto nos negócios causados por quaisquer dados corrompidos.

A autenticação de mensagens é uma técnica usada para detectar alterações não autorizadas dos conteúdos de uma mensagem transmitida electronicamente. Ela pode ser implementada em hardware ou software que suporte um dispositivo físico de autenticação de mensagens ou um algoritmo de software.

A autenticação de mensagens deve ser considerada para aplicativos onde exista uma necessidade de segurança para proteger a integridade do conteúdo das mensagens.

A saída de dados de um sistema aplicativo deve ser validada para garantir que o processamento de informações armazenadas seja correcto e apropriado às circunstâncias. Geralmente, os sistemas são construídos baseados na premissa de que tendo havido validação apropriada, confirmação e testes, a saída será sempre correcta.

Controlos criptográficos

O objectivo é proteger a confidencialidade, autenticidade ou integridade das informações.

Sistemas e técnicas criptográficas devem ser usados para a protecção das informações que estejam consideradas em risco e para as quais outros controlos não propiciam protecção adequada.

A tomada de decisão sobre se uma solução criptográfica é apropriada deve ser vista como uma parte de um processo mais amplo de avaliação de riscos e selecção de controlos. Uma avaliação de riscos deve ser efectuada para determinar o nível de protecção que as informações devem receber. Esta avaliação pode então ser usada para determinar se um controlo criptográfico é apropriado, que tipo de controlo deve ser aplicado e para quais propósitos e processos do negócio.

Uma organização deve desenvolver uma política sobre o uso de controlos criptográficos para protecção das suas informações. Uma tal política é necessária para maximizar os benefícios e minimizar os riscos de usar técnicas criptográficas, e evitar uso inapropriado ou incorrecto.

A criptografia é uma técnica que pode ser usada para proteger a confidencialidade das informações. Deve ser considerada para protecção de informações sensíveis ou críticas.

O nível requerido de protecção deve ser identificado com base numa avaliação de riscos, tendo em conta o tipo e a qualidade do algoritmo de criptografia usado bem como o tamanho das chaves criptográficas a serem utilizadas.

Ao se implementar a política de criptografia da organização, devem ser considerados os regulamentos e as restrições nacionais que se podem aplicar ao uso de técnicas criptográficas em diferentes partes do mundo e às questões de fluxo de informação criptográfica entre países.

As assinaturas digitais fornecem um meio de proteger a autenticidade e a integridade de documentos electrónicos. Por exemplo, eles podem ser usados no comércio electrónico, onde

houver necessidade de confirmar quem assinou um documento electrónico e de verificar se os conteúdos do documento assinado foram alterados (timestamp).

As assinaturas digitais podem ser aplicadas a qualquer forma de documento processado electronicamente. A sua implementação pode ser feita através de uma técnica criptográfica baseada num par de chaves relacionadas de forma única, onde uma chave é usada para criar a assinatura e a outra para verificar a assinatura.

Serviços de não-rejeição

Devem ser utilizados serviços de não-rejeição, para resolver disputas sobre a ocorrência ou não ocorrência de um evento ou acção. Eles podem ajudar a estabelecer provas para substanciar se um determinado evento ou acção ocorreu, por exemplo negação de envio de uma instrução assinada electronicamente usando correio electrónico. Estes serviços são baseados no uso de técnicas de criptografia e assinatura digital.

A gestão das chaves criptográficas é essencial para o uso eficaz das técnicas de criptografia.

Um sistema de gestão de chaves deve ser baseado num conjunto acordado de padrões, procedimentos e métodos seguros.

Segurança de arquivos do sistema

O objectivo é assegurar que os projectos de IT e actividades de suporte sejam conduzidos de uma forma segura. O acesso aos arquivos do sistema deve ser controlado.

Manter a integridade do sistema deve ser responsabilidade da função usuária ou grupo de desenvolvimento ao qual o sistema aplicativo ou software pertence.

Deve ser fornecido controlo para a implementação de software em sistemas operacionais.

O software usado em sistemas operacionais, que seja fornecido pelo revendedor, deve ser mantido num nível no qual o fornecedor dá suporte. Qualquer decisão de fazer *upgrade* para uma nova versão deve ter em conta a segurança da versão, isto é, a introdução de uma nova funcionalidade de segurança ou a quantidade e a severidade dos problemas de segurança que afectam esta versão.

Os dados de teste devem ser protegidos e controlados. Os testes e a aceitação de sistemas geralmente exigem volumes substanciais de dados de teste que sejam o mais parecido possível com os dados operacionais. O uso de bancos de dados operacionais contendo informações pessoais deve ser evitado. Se tais informações forem usadas, elas devem ser despersonalizadas antes do uso. Os seguintes controlos devem ser aplicados para proteger dados operacionais:

Segurança nos processos de desenvolvimento e suporte

O objectivo é manter a segurança dos softwares e das informações dos sistemas aplicativos. Os ambientes de projecto e suporte devem ser estritamente controlados. Os gestores

responsáveis pelos sistemas aplicativos também devem ser responsáveis pela segurança do ambiente de projecto ou suporte. Eles devem assegurar que todas as alterações propostas nos sistemas sejam revistas para verificar se elas não comprometem a segurança do sistema ou do ambiente operacional.

Procedimentos para controlo de alterações

Para minimizar o rompimento dos sistemas de informação, deve existir um controlo estrito sobre a implementação de alterações. Devem ser obrigatórios procedimentos formais para controlo de alterações. Eles devem garantir que os procedimentos de controlo e segurança não sejam comprometidos, que os programadores do suporte recebam acesso apenas àquelas partes do sistema necessárias para o trabalho, e que sejam obtidos um acordo e uma aprovação formais para cada alteração. Alterar software aplicativo pode causar impacto no ambiente operacional.

Periodicamente, é necessário alterar o sistema operacional.

Devem ser desencorajadas modificações em pacotes de software. Tanto quanto possível, e praticável, os pacotes de software fornecidos por revendedor devem ser usados sem modificação.

Um "***covert channel***" pode expôr informação através de alguns meios indirectos e obscuros.

Ele pode ser activado alterando-se um parâmetro acessível tanto por elementos seguros quanto inseguros de um sistema informatizado, ou embutindo-se informação num fluxo de dados. O código troiano é projectado para afectar um sistema de uma forma que não é autorizada, não é prontamente percebida e não é solicitada pelo receptor ou utilizador de um programa. "***Covert channels***" e código troiano raramente ocorrem por acidente.

6.1.9 Gestão da continuidade de negócio

Aspectos da gestão da continuidade do negócio

O seu objectivo é anular interrupções nas actividades do negócio e proteger processos críticos do negócio contra os efeitos de grandes falhas ou desastres.

Um processo de gestão da continuidade do negócio deve ser implementado para reduzir a perturbação causada por desastres e falhas de segurança a um nível aceitável através da combinação de controlos preventivos e de recuperação.

Devem ser desenvolvidos e implementados planos de contingência para assegurar que os processos do negócio possam ser restaurados dentro dos limites temporais exigidos. Tais planos devem ser actualizados e praticados para se tornarem uma parte integral de todos os outros processos de gestão.

A continuidade do negócio deve começar pela identificação de eventos que possam causar interrupções nos processos do negócio, tais como falhas em equipamento, incêndios e inundações. Isto deve ser seguido por uma avaliação de riscos para determinar o impacto daquelas interrupções, tanto em termos de escala de danos como de período para recuperação. Ambas as actividades devem ser executadas com o total envolvimento dos proprietários dos recursos e processos do negócio. Esta avaliação considera todos os processos do negócio e não é limitada às facilidades de processamento de informação.

Deve ser desenvolvido um plano estratégico para determinar o enfoque global para a continuidade do negócio. Uma vez criado este plano, ele deve ser endossado pela gestão. Devem ser desenvolvidos planos para manter ou restaurar as operações do negócio nos limites temporais exigidos seguintes à interrupção, ou falha, nos processos críticos do negócio.

Deve ser mantida uma única estrutura para os planos de continuidade do negócio, para garantir que todos os planos sejam consistentes e para identificar prioridades para os testes e para a manutenção. Cada plano de continuidade do negócio deve especificar claramente as condições para sua activação, bem como os indivíduos encarregados pela execução de cada componente do plano. Quando forem identificados novos requisitos, os procedimentos de emergência estabelecidos, tais como planos de evacuação ou quaisquer arranjos de ***fallback*** existentes, devem ser ajustados conforme apropriado. Os planos para continuidade do negócio podem falhar ao serem testados, frequentemente devido a suposições incorrectas, omissões ou mudanças em equipamentos ou pessoal. Portanto, devem ser testados regularmente para assegurar que são actualizados e eficazes. Tais testes também devem garantir que todos os membros da equipa de recuperação e outras equipas relevantes estejam cientes dos planos.

O cronograma de testes para o(s) plano(s) para continuidade do negócio deve indicar como e quando cada elemento do plano deve ser testado.

Diversas técnicas devem ser usadas para garantir que os planos funcionarão na vida real. Estas técnicas podem incluir por exemplo, testes de mesa de diversos cenários (discutir os arranjos para recuperação usando interrupções de exemplo); simulações; testes da recuperação técnica; testar recuperação num *site* alternativo; testes das facilidades e serviços de fornecimento e ensaios.

As técnicas podem ser usadas por qualquer organização e devem reflectir a natureza do plano de recuperação específico.

Os planos para continuidade do negócio devem passar por revisões e actualizações regulares para garantir uma eficácia continuada. Devem ser incluídos procedimentos dentro do programa de gestão de mudanças da organização para garantir que as questões relacionadas com a continuidade do negócio são tratadas adequadamente.

Deve ser atribuída responsabilidade pelas revisões regulares de cada plano para continuidade do negócio; a identificação de mudanças nos arranjos comerciais ainda não

reflectidas nos planos para continuidade do negócio deve ser seguida por uma actualização adequada do plano.

6.1.10 Obediência a exigências

Obediência às exigências legais

O objectivo é evitar a infracção de qualquer lei civil e criminal, estatutária, regulamentadora ou de obrigações contratuais e de quaisquer requisitos de segurança.

O projecto, operação, uso e gestão de sistemas de informação podem estar sujeitos a exigências de segurança estatutárias, regulamentadoras e contratuais.

Deve ser procurado aconselhamento sobre exigências legais específicas com os consultores jurídicos da organização, ou profissionais adequadamente qualificados. As exigências da legislação variam de país para país e de acordo com a informação gerada num país e transmitida para outro país (por exemplo, fluxo de dados entre países).

Todas as exigências contratuais, estatutárias e regulamentadoras relevantes devem ser explicitamente definidas e documentadas para cada sistema de informação. Os controlos específicos e as responsabilidades individuais para satisfazer estas exigências devem estar similarmente definidos e documentados.

Os procedimentos apropriados devem ser implementados para garantir o cumprimento de restrições legais quanto ao uso de material em relação ao qual podem existir direitos de propriedade intelectual, tais como *copyright*, direitos de projecto e marcas registadas.

As exigências legislativas, regulamentadoras e contratuais podem colocar restrições quanto à cópia de material proprietário. Em particular, elas podem obrigar que apenas material que é desenvolvido pela organização, ou que é licenciado ou fornecido pelo investigador para a organização, possa ser usado.

Os produtos proprietários de software são geralmente fornecidos com um contrato de licenciamento que limita o uso dos produtos a máquinas especificadas e pode permitir cópias apenas para a criação de ***backups***.

Os Registos importantes de uma organização devem ser protegidos contra perda, destruição e falsificação. Alguns registos podem precisar de ser guardados em segurança para satisfazer exigências estatutárias ou regulamentadoras, bem como para apoiar actividades essenciais do negócio. Exemplos destes são registos que podem ser exigidos como prova de que uma organização opera dentro das normas estatutárias ou regulamentadoras, ou para assegurar defesa adequada contra potencial acção criminal ou civil, ou para confirmar o status financeiro de uma organização com respeito a accionistas, parceiros e auditores. O período de tempo e os conteúdos de dados para retenção das informações podem ser definidos por lei ou regulamento nacional.

Os sistemas de armazenamento de dados devem ser escolhidos de forma que os dados exigidos possam ser recuperados de uma forma aceitável num tribunal. O sistema de armazenamento deve garantir a identificação clara dos registos e de seu período de retenção estatutário ou regulamentar. Ele deve permitir a destruição apropriada dos registos após aquele período se eles não forem necessários para a organização.

Diversos países introduziram legislação que coloca controlos no processamento e transmissão de dados pessoais.

Tais controlos podem impor obrigações para aqueles que colectam, processam e disseminam informações pessoais, e podem restringir a capacidade de transferir aqueles dados para outros países.

A obediência à legislação de protecção de dados exige estrutura de gestão e controlo apropriadas. Com frequência, a melhor forma de conseguir isto é pela nomeação de um encarregado da protecção dos dados, que deve fornecer orientação para os gerentes, utilizadores e provedores de serviço sobre as suas responsabilidades individuais e os procedimentos específicos que devem ser seguidos. Deve ser responsabilidade dos proprietários dos dados informar o encarregado da protecção aos dados sobre quaisquer propostas para manter informações pessoais num arquivo estruturado e para assegurar a consciencialização sobre os princípios de protecção dos dados definidos na legislação relevante.

As facilidades de processamento de informação de uma organização são fornecidas para os fins do negócio. A gestão deve autorizar o seu uso. Qualquer utilização destas facilidades para propósitos não autorizados ou não relacionados ao negócio, sem aprovação da gestão, deve ser considerada como uso impróprio das facilidades.

Muitos países têm, ou estão em processo de implantação, legislação para proteger contra a má utilização de computadores.

Alguns países implementaram acordos, leis, regulamentos ou outros instrumentos para controlar o acesso a controlos criptográficos ou o seu uso.

É necessário ter provas adequadas para apoiar uma acção contra uma pessoa ou organização. Sempre que esta acção for uma questão disciplinar interna, a prova necessária estará descrita pelos procedimentos internos.

Para obter a admissibilidade da prova, as organizações devem assegurar-se de que os seus sistemas de informação obedecem a algum padrão ou código de prática publicado sobre produção de prova admissível.

Para obter qualidade da prova, é necessário um sólido rastreamento da prova.

Revisões da política de segurança e obediência técnica

O objectivo é garantir a obediência dos sistemas às políticas e padrões de segurança da organização.

A segurança de sistemas de informação deve ser revista regularmente.

Os gestores devem assegurar que todos os procedimentos de segurança dentro das suas áreas de responsabilidade são executados correctamente.

Os sistemas de informação devem ser verificados regularmente quanto à obediência aos padrões de implementação de segurança. A verificação da obediência técnica envolve o exame de sistemas operacionais para garantir que os controlos de hardware e software foram correctamente implementados. Este tipo de verificação de obediência exige assistência técnica especializada. Deve ser executada manualmente por um engenheiro de sistemas experiente, ou por um pacote de software automatizado que gere um relatório técnico para subsequente interpretação por um especialista técnico.

A verificação da obediência cobre também, por exemplo, testes de penetração, que podem ser executados por especialistas independentes contratados especificamente para este propósito. Isto pode ser útil para detectar vulnerabilidades no sistema e para verificar quão eficazes os controlos são na prevenção de acesso não autorizado devido a estas vulnerabilidades. Deve-se exercer cautela no caso de um sucesso em testes de penetração poder levar a um compromisso da segurança do sistema e inadvertidamente explorar outras vulnerabilidades.

Considerações para auditoria de sistemas

O objectivo é maximizar a eficácia do processo de auditoria de sistemas, minimizar a interferência do processo de auditoria nos negócios e minimizar interferências no processo de auditoria.

Devem existir controlos para salvaguardar os sistemas operacionais e as ferramentas de auditoria durante auditorias de sistemas.

Os requisitos de auditoria e actividades envolvendo verificações em sistemas operacionais devem ser cuidadosamente planeados e acordados para minimizar o risco de perturbações nos processos do negócio.

6.2 Família ISO 27000

6.2.1 O que é

A norma ISO 27000 está relacionada com o vocabulário da gestão segurança de informação.

6.2.2 Composição

Para além da **ISO 27000** é constituída pela **ISO 27001**, publicada em Outubro de 2005 e que substituiu a norma BS 7799-2 para certificação de sistema de gestão de segurança da informação; pela **ISO 27002**, este standard substituiu em 2006/2007 a já mencionada ISO 17799:2005 (Código de Boas Práticas); a **ISO 27003**, aborda a gestão de risco, contendo recomendações para a definição e implementação de um sistema de gestão de segurança da

informação; a **ISO 27004** Incide sobre os mecanismos de mediação e de relatório de um sistema de gestão de segurança da informação; a **ISO 27005** é constituída por indicações para implementação, monitorização e melhoria contínua do sistema de controlos. O seu conteúdo é idêntico ao da norma BS 7799-3:2005 – "Information Security Management Systems - Guidelines for Information Security Risk Management" e a **ISO 27006**, está dentro da série 27000 e é a última norma, que é referente à recuperação e continuidade de negócio.

6.3 Norma ISO 27001[32]

6.3.1 Introdução à Norma

Trata-se (de acordo com Francesco[33] de Cicco), de uma especificação de um Sistema de Gestão da Informação composto por sete secções:

0) Introdução
1) Objectivo e Campo de Aplicação
2) Referências Normativas
3) Termos e Definições
4) Sistema de Gestão da Segurança da Informação
5) Responsabilidades da Direcção
6) Análise Crítica do SGSI
7) Melhoria do SGSI

Definindo também um processo de seis etapas para a implementação desse SGSI:

i. Definição da política de segurança da informação da organização;
ii. Definir o âmbito do SGSI;
iii. Identificar, analisar e avaliar os riscos;
iv. Tratar os riscos avaliados;
v. Seleccionar os controlos a implementar;
vi. Preparar uma declaração de aplicabilidade.

6.3.2 Processo de abordagem

O processo de abordagem para a gestão da segurança da informação apresentado nesta norma tem ênfase nos seguintes factores:

1. A compreensão dos requisitos de segurança da informação de uma organização e a necessidade do estabelecimento de políticas e objectivos relativos à segurança da informação;

[32] *In* ISO (2005). ISO 27001. Suiça, ISO. **27001.**
[33] *In* Cicco, F.(2006)ISO/IEC 27001 na opinião de um especialista.3

2. Implementar e trabalhar comandos para gerir os riscos de segurança da informação de uma organização no contexto dos riscos globais de negócio da organização;
3. Vigiar e rever o desempenho e eficácia dos Sistemas de Gestão da Segurança da Informação;
4. Melhoria contínua com base em medições objectivas.

Esta Norma Internacional adoptou o modelo do Plan-Do-Check-Act, o qual é aplicado à estrutura de todos os processos dos Sistemas de Gestão de Segurança da Informação.

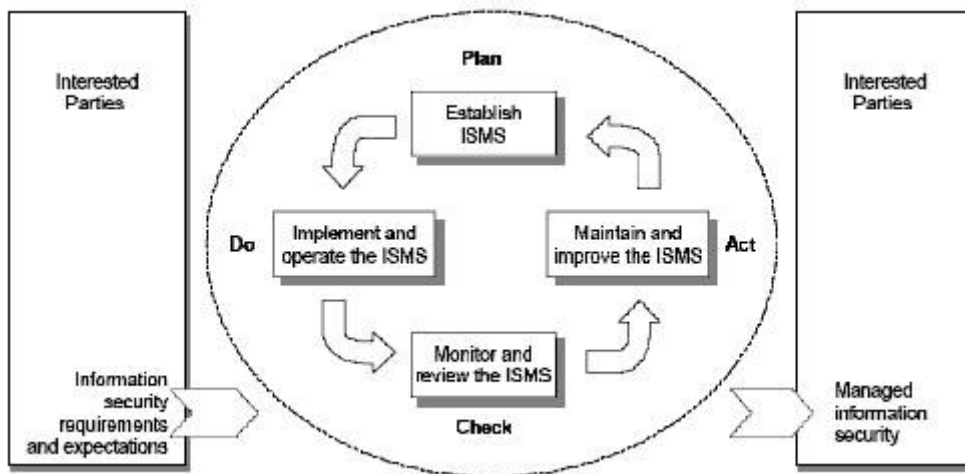



Ilustração 3:Plan-Do-Check-Act in Norma 27001

Passemos à descrição das várias etapas do plano:

Plan: estabelece as políticas dos sistemas de gestão de segurança da informação, objectivos, processos e procedimentos importantes para gerir o risco e melhorar a segurança da informação, para que sejam atingidos resultados adequados às políticas da organização e aos seus objectivos.

Do (efectuação e gestão do SGSI): efectua e gere as políticas, controlos, processos e procedimentos do SGSI.

Check (vigiar e rever o SGSI): aceder e medir a reacção do processo relativamente às políticas do Sistema de Gestão de Segurança da Informação, objectivos e experiência prática e expor os resultados da gestão a uma revisão.

Act (manter e melhorar o Sistema de Gestão da Informação): desenvolver acções correctivas e preventivas com base nos resultados de auditorias internas ao Sistema de Gestão de Segurança da Informação e gerir revisões ou outras informações importantes para que se obtenha uma melhoria continua do Sistema de Gestão de Segurança da Informação.

6.3.3 Âmbito/abrangência da norma

Esta Norma Internacional abrange todos os tipos de organizações, e especifica os requisitos para estabelecer, implementar, vigiar, operar, rever, manter e melhorar um Sistema de

Gestão de Segurança da Informação documentado e inserido no contexto dos riscos globais de negócio da organização. Esta Norma define os requisitos para a implementação dos controlos de segurança adaptados às necessidades da organização ou de partes que a compõem.

O Sistema de Gestão de Segurança da Informação tem como função assegurar a selecção de controlos de segurança adequados à protecção do acesso à informação e à manutenção da confidencialidade das partes interessadas.

É necessário justificar qualquer exclusão de controlos determinada como necessária para satisfazer os necessários critérios de aceitação de risco, e tem de ser provado que os riscos associados são aceites pelas pessoas implicadas.

6.3.4 Sistemas de Gestão de Segurança da Informação

Os sistemas de gestão da segurança da informação são colocados em prática através do já especificado Plan Do Check Act.

Estabelecimento e gestão do SGSI

1.a) Estabelecendo o SGSI

O primeiro passo é sem dúvida a implementação do Sistema de Gestão de Segurança da Informação. Para isso, a organização deve proceder à realização de algumas etapas, a saber:

a) DEFINIR A COBERTURA E AS DELIMITAÇÕES DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO no que respeita à caracterização do negócio, à organização, à sua localização, tecnologia, acessos á informação, eventuais detalhes considerados relevantes, e (se for caso disso), as exclusões feitas á cobertura da Norma, acompanhadas da respectiva justificação;
b) DEFINIR UMA POLÍTICA DE SISTEMAS DE GESTÃO DA INFORMAÇÃO, com ênfase em pontos como: características do negócio, da organização, sua localização, tecnologia e acesso, tendo em conta os seguintes parâmetros:
    1) Enquadrar a definição de objectivos e delinear os princípios de acção que regem a segurança da informação;
    2) A área de negócio e os requisitos legais ou regulamentares e as obrigações de segurança acordadas em contrato;
    3) O alinhamento com a estratégia de gestão de risco da organização e o contexto no qual o Sistema de Gestão de Segurança da Informação irá ser implementado;
    4) Estabelecer condições a seguir para a avaliação do risco;

5) Zelar para que a política do Sistema de Gestão de Segurança da Informação implementado tenha sido aprovada pela gestão de topo.

c) DEFINIR A ESTRATÉGIA DE AVALIAÇÃO DE RISCO DA ORGANIZAÇÃO:
   1) Identificar uma metodologia de avaliação de risco apropriada ao Sistema de Gestão de Segurança da Informação e aos requisitos de negócio (legais e regulamentares) identificados para a segurança da informação;
   2) Desenvolver condições para que os riscos sejam aceites e identificar os níveis de risco aceitáveis;
   3) A metodologia de avaliação de riscos enunciada deve assegurar que a avaliação de riscos produz resultados comparáveis e reprodutíveis.

d) IDENTIFICAÇÃO DOS RISCOS:
   1) Identificar tanto os ‘bens’ abrangidos pelo Sistema de Gestão de Segurança da Informação como os proprietários desses ‘bens’;
   2) Identificar as ameaças a esses ‘bens’;
   3) Identificar os pontos vulneráveis susceptíveis de serem explorados por essas ameaças;
   4) Identificar o impacto que a perda de confidencialidade, integridade e disponibilidade podem representar para esses ‘bens’;

e) ANALISE E AVALIAÇÃO DOS RISCOS:
   1) Avaliar o impacto que uma falha de segurança poderá ter no negócio de uma organização, tendo em conta as eventuais consequências de perda de confidencialidade, integridade e disponibilidade da informação;
   2) Avaliar de forma realista a probabilidade de uma falha de segurança acontecer devido às vulnerabilidades do sistema e os impactos associados aos ‘bens’ e às formas de controlo actualmente em vigor;
   3) Avaliar os níveis de risco;
   4) Determinar até que ponto o risco é aceitável e a partir de que momento é necessário utilizar um tratamento através das condições de aceitação de risco estabelecidas em 2.a. 1c) 2).

f) IDENTIFICAR E AVALIAR AS OPÇÕES PARA O TRATAMENTO DE RISCOS:
   1) Aplicar controlos adequados;
   2) Aceitar os riscos de forma consciente e objectiva, atendendo à plena satisfação das políticas da organização e às condições para que os riscos sejam aceitáveis;
   3) Evitar os riscos;
   4) Transferir os riscos associados ao negócio para outras partes interessadas, como por exemplo os fornecedores;

g) SELECCIONAR OBJECTIVOS DE CONTROLO E CONTROLOS PARA O TRATAMENTO DE RISCO:
   1) Os objectivos de controlo e controlos devem ser seleccionados e colocados em prática com o objectivo de satisfazer os requisitos identificados pela avaliação de riscos e pelo processo de tratamento de risco. Para isso, devem ser levadas em linha de conta não só as condições de aceitação de risco, mas também os requisitos legais, regulamentares e contratuais;
   2) Os objectivos de controlo e controlos presentes no Anexo A da Norma ISO 27001 (ver Anexo 2) devem ser seleccionados como parte deste processo, e entendidos como satisfatórios para abranger esses requisitos. Trata-se de objectivos de controlo incompletos, que podem ser destacados como objectivos de controlo ou controlos complementares.

h) OBTER APROVAÇÃO PARA OS RESTANTES RISCOS PROPOSTOS;
i) OBTER AUTORIZAÇÃO PARA IMPLEMENTAR E COLOCAR OPERACIONAL O SGSI;
j) PREPARAR UMA DECLARAÇÃO DE APLICABILIDADE QUE COMPREENDA:
   1) Os objectivos de controlo e os controlos seleccionados em 2.a.1.g), bem como os motivos que levaram a essa selecção;
   2) Os objectivos de controlo e os controlos actualmente implementados na organização;
   3) A exclusão de quaisquer objectivos de controlo e controlos presentes no Anexo A, acompanhada da devida justificação.

1.b) Implementar e trabalhar o SGSI:

Esta etapa é composta por oito passos distintos a realizar pela organização:

a) Conceber um plano de tratamento de risco que identifique a acção de gestão adequada, recursos, responsabilidades e prioridades na gestão dos riscos de segurança da informação;
b) Colocar em prática um plano de tratamento de risco para atingir os objectivos de controlo que incluem os financiamentos e a distribuição de papéis e de responsabilidades numa organização;
c) Implementar os controlos seleccionados de forma a atingir os objectivos de controlo;
d) Definir como medir a eficácia dos controlos ou grupos de controlos seleccionados e especificar como essas medidas devem ser utilizadas para avaliar a eficácia do controlo na produção de resultados passíveis de serem comparados e reproduzidos;
e) Promover programas de treino e de consciencialização;
f) Gerir operações de SGSI;

g) Gerir recursos de SGSI;
h) Colocar em prática procedimentos e outros controlos que permitam detectar e responder rápida e eficazmente a incidentes de segurança.

1.c) Monitorizar e rever o SGSI:

Por sua vez, esta etapa é composta por sete passos, sendo alguns deles decompostos em sub-etapas.

a) Executar a vigilância e revisão de procedimentos e outros controlos, com o objectivo de:
    1) Detectar rapidamente possíveis erros no resultado dos procedimentos;
    2) Identificar atempadamente e com sucesso lacunas e incidentes de segurança;
    3) Permitir à gestão determinar se as actividades de segurança sob a responsabilidade de pessoas ou postas em prática através de tecnologias de informação, estão a ser devidamente executadas;
    4) Ajudar a detectar problemas de segurança e assim prevenir incidentes de segurança através da utilização de indicadores;
    5) Determinar a eficácia das acções levadas a cabo para solucionar uma eventual falha de segurança;
b) Rever periodicamente a eficácia do SGSI tendo em conta os resultados de auditorias, incidentes, eficácia das medidas, sugestões e feedback das partes envolvidas – relativamente à informação;
c) Medir a eficácia dos controlos para verificar se foram seguidos os requisitos de segurança;
d) Rever periodicamente a avaliação de riscos e rever o nível de riscos residuais e os riscos aceitáveis identificados, considerando mudanças de:
    1) A organização;
    2) Tecnologia;
    3) Objectivos e processos de negócio;
    4) Identificar ameaças;
    5) Eficácia dos controlos colocados em prática;
    6) Eventos externos, tais como: alterações no meio legal ou regulamentar, alterações às obrigações contratuais e alterações no meio social;
e) Dirigir auditorias internas ao SGSI seguindo intervalos periódicos;
f) Responsabilizar-se pelas gestões de revisão do SGSI de acordo com uma base regular para garantir que o âmbito da norma continua a ser apropriado e se são identificadas as melhorias nos processos de SGSI;

g) A actualização dos planos de segurança tendo em conta as descobertas nas actividades de monitorização e revisão;
h) Registar acções e eventos passíveis de causar impacto na eficácia ou desempenho do SGSI;

1.c) Manter e melhorar o SGSI:

A organização deve tomar regularmente as seguintes medidas:

a) Pôr em prática as melhorias identificadas no SGSI;
b) Levar a cabo acções preventivas e correctivas adequadas de acordo com os pontos 6.a e 6.b. Aplicar as lições apreendidas de experiências de segurança de outras organizações e aquelas da própria organização;
c) Comunicar as acções e melhorias a todas as partes interessadas na eficácia do desempenho do SGSI;

a. Requisitos de documentação:

1.a) Geral:

Os documentos necessários para o SGSI são:

a) Declarações documentadas da política e dos objectivos de SGSI (ver 2.a.1c));
b) O âmbito do SGSI;
c) Procedimentos e controlos de apoio ao SGSI;
d) A descrição da metodologia de avaliação de riscos;
e) O registo de avaliação de riscos;
f) O plano de tratamento de risco;
g) Procedimentos documentados exigidos pela organização para garantir a efectividade do plano, organização e controlo dos processos de segurança de informação e descrever como medir a eficácia dos controlos;
h) Registos exigidos por esta Norma;
i) Declaração de aplicabilidade.

1.b) Controlo de Documentos:

1.a) Controlo de Registos:

6.3.5 Gestão de responsabilidade

a. Compromissos de gestão

b. Gestão de recursos

a) Fornecimento de recursos;
b) Treino, consciencialização e competência;

6.3.6 Auditorias internas ao SGSI

6.3.7 Gerir a revisão do SGSI

a. *Geral;*

b. *Revisão das entradas;*

c. *Revisão das saídas;*

6.3.8 Melhoria do SGSI

a. *Melhoria continua*
b. *Acções correctivas*

Esta etapa está relacionada com acções que devem ser desenvolvidas pela organização com o objectivo de eliminar as inconformidades existentes relativamente às exigências do SGSI.

c. *Acções preventivas*

Acções preventivas são acções levadas a cabo pela organização para eliminar causas de eventuais inconformidades com os requisitos do SGSI.

Em jeito de conclusão, pode afirmar-se que, tal como Francesco de Cicco[34], a adopção desta Norma por parte das empresas representa uma vantagem, que é o facto de tornar evidente não só para os clientes como para os fornecedores, que a organização está de facto a levar a sério a segurança da informação, uma vez que as organizações enfrentam ameaças e riscos de segurança através de processos actualizados. Este autor está ainda de acordo com a Norma quando afirma que o Sistema de Gestão da Segurança da Informação, enquanto abordagem sistémica para gerir as informações importantes da empresa, necessita do envolvimento de todos os colaboradores e dos processos de Sistemas de Tecnologias de Informação.

6.4 Complementaridade entre as normas ISO 17799 e ISO 27001

São duas normas que apesar de distintas se complementam. Tratando-se a Norma 17799 de um código de práticas para gerir a segurança da informação, e dedicando-se a Norma ISO 27001 ao fornecimento de um modelo com o objectivo de estabelecer, implementar, operar, monitorizar, rever, manter e melhorar o Sistema de Gestão de Segurança da Informação, estas duas normas acabam por funcionar de uma forma encadeada e interdependente. É aliás usual que uma organização que se baseie na Norma ISO 27001 para implementar um Sistema de Gestão de Segurança da Informação siga também as práticas instituídas pela Norma 17799.

[34] *In* Cicco, F.(2006)ISO/IEC 27001 na opinião de um especialista.3

No entanto, de acordo com Francesco de Cicco[35], parece ter-se gerado alguma confusão em torno da Norma ISO 17799, uma vez que ao contrário do que muitas vozes afirmam, tratando-se desta Norma de um documento que 'aponta caminhos' e princípios gerais para melhorar a segurança da informação nas organizações, não deve ser utilizada com a finalidade de certificação. Segundo o autor, "A ISO 17799 é, portanto, um código de boas práticas que se complementa de forma excelente com a Norma ISO 27001".

6.5 De que forma as normas contribuem para garantir a segurança da informação?

Embora as normas nem sempre sejam passíveis de ser utilizadas pelas instituições, e a sua eficácia não corresponda a 100%, são instrumentos que (quando adoptados), permitem às instituições ultrapassar muitas vulnerabilidades relacionadas com a segurança da informação. Desta forma, tornam-se mais eficazes no combate à informação, e inspiram mais confiança aos utilizadores, o que potencia o seu sucesso.

7 Políticas de segurança da informação

7.1 Questões de segurança nacional relacionadas com a segurança da informação (resposta dos governos)

Como consequência do desenvolvimento da informatização, os problemas de segurança da informação como emails *spam, phishing e pharming* as ameaças á infra-estrutura nacional, têm aumentado. Como a rede de infra-estrutura nacional foi desenvolvida e difundida, a informação foi igualmente partilhada e intercambiada, e o acesso ilegal à informação tornou-se um sério problema. À medida que a comunicação em rede é transformada num sistema global internacional, a resposta legal às invasões estranhas e aos ciber-ataques está a atingir o seu limite. Numa perspectiva internacional, num ambiente onde as maiores infra-estruturas são geridas e controladas com base na informação da comunicação em rede, alguns problemas constituem uma séria ameaça à segurança nacional.

A fim de solucionar esta questão, muitas nações em todo o mundo têm-se dedicado à pesquisa e ao desenvolvimento de várias técnicas e políticas de segurança da informação[36],

[35] *In* Cicco, F.(2006)ISO/IEC 27001 na opinião de um especialista.3

[36] *In* Yoo, Don-Young; Shin, Jong-Whoi; Lee, Gang-Shin, et al. (2007). "Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)." PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY: 6.

assumidas como esforços governamentais para proteger as suas infra-estruturas de novas e emergentes ameaças. Nos Estados Unidos, foi promulgado em 1996, o *National Information Infrastructure Protection Act*, e em Maio de 1998, foi emitida a *Presidential Decision Directive (PDD) 63*, para criar todo um sistema de segurança governamental para as maiores infra-estruturas, é importante referir que esse plano foi concebido para ser colocado em prática no ano 2000 e estar a funcionar na sua plenitude em 2003[37]. Para além disso, foi fundado, com a emissão da Executive Order-13284 em Janeiro de 2003, o Department of Homeland Security (DHS), e em Fevereiro de 2003 foi anunciada uma iniciativa de estratégia nacional para a segurança no ciberespaço.

Em Fevereiro de 2000, o Japão administrou leis contra actos de acesso ilegal e estabeleceu o Comité de Medidas de Segurança e o Civilian Experts Council no Centro Estratégico de Informação Tecnológica. Também a Coreia estabeleceu, em conformidade com a lei de infra-estrutura de segurança promulgada em 2001, o comité de infra-estruturas de segurança, e tem vindo a construir, de forma sistemática e compreensiva, medidas contra o ataque electrónico para importantes infra-estruturas de informação e telecomunicação. Desde que a protecção para o controlo e operação de maiores infra-estruturas sociais requer o envolvimento de factores, como: comunicação, financeiro, militar e energético - o comité foi fundado pelo primeiro-ministro Coreano para dirigir e coordenar o estabelecimento e a execução de políticas de segurança de infra-estruturas de informação e telecomunicação.

Contudo, as políticas de segurança, têm usualmente sido estabelecidas sem ter em conta os níveis de segurança. Por isso, com o objectivo de estabelecer uma política de segurança mais eficaz, têm de ser desenvolvidas metodologias que assegurem o nível de segurança baseado na vulnerabilidade e no resultado das análises. Kenneth J. Knapp, Thomas E. Marshall, R. Kelly Rainer, Jr., e Dorsey W. Morrow, através do seu artigo *The Top Information Security Issues Facing Organizations: What Can Government do to Help?*[38], reforçam a necessidade dos governos – mais concretamente o governo dos EUA – criarem um ambiente legislativo que proteja as empresas dos ataques à segurança da informação.

8 Metodologia de avaliação da segurança de informação

A necessidade do desenvolvimento de uma Metodologia de partilha de informação advém do facto das políticas de segurança serem implementadas ignorando os níveis de

---

[37] *In* Ott, J. L. (2000). "Information Security in the New Millenium." Information Security Journal **9**(1): 3.

[38] *In* Knapp, K; Marshall, T.; JR. Rainer, R. K., et al. (2006). "The Top Information Security Issues Facing Organizations: What Can Government Do to Help?" Information Security Journal **15**(4): 8.

segurança, e sentindo-se uma necessidade emergente de aumentar a eficácia das políticas de segurança, verificou-se o desenvolvimento de metodologias, que baseadas na vulnerabilidade e no resultado das análises aos sistemas de segurança, garantam o nível de segurança. No seu artigo *Improve of Evaluation Method of Information Security Levels of CIIP, Yoo, Shin, Lee e Lee (Yoo, Shin, Lee e Lee, 2007*, apresentam-nos um Método, segundo eles capaz de proporcionar esquemas e métodos de avaliação susceptíveis de serem utilizados para melhorar o nível de segurança de uma forma continua e activa. Esse método é denominado de *Information Security Evaluation Method*.

8.1 Information Security Evaluation Method

Este método compõem-se por procedimentos destinados a medir o nível de segurança da organização, e, através da análise dos dados, determina a maturidade desse nível de segurança. Trata-se de um método desenvolvido com o objectivo de detalhar os parâmetros de avaliação presentes na BS 7799[39], entre outras Normas. A avaliação da segurança dos diversos níveis é feita através de 12 categorias, 54 itens e 89 detalhes de controlo. Estes últimos dividem-se ainda em 41 itens correspondentes a processos, e 49 itens denominados de itens funcionais. Enquanto os itens funcionais estão relacionados apenas com a provisão de funções, os itens de processos podem ser classificados como sub-processos. Para avaliar as 12 categorias de controlo e os 89 detalhes de controlo de itens, é elaborada uma lista de verificação, divisível em cinco níveis. Essa lista é passível de ser utilizada para uma auto-avaliação por parte da organização, cujo resultado é certificado através da inspecção de documentos relacionados, de inspecções no local e da análise de gestores.

O resultado do nível de protecção da informação de uma organização pode ser avaliado através de dois métodos:

1. Cálculo da maturidade do resultado do nível de protecção da informação através da soma dos valores da avaliação dos detalhes de controlo de itens para os 54 itens de controlo:

$$S = \sum_{i=0}^{n} L_i$$

(1)

(S: itens de controlo, i L : detalhe de controlo de item)

A primeira etapa da avaliação dos detalhes de controlo de itens é calculada tendo por base o patamar mais baixo da informação, e tendo como referencia a maturação da protecção do

[39] Que serviu de base para a criação da Norma ISO 17799

nível. O nível de avaliação é a soma total dos valores de avaliação dos detalhes de controlo de itens sob o número de detalhes de itens de avaliação.

$$AL = \frac{S}{N\ itens} \quad (2)$$

(S: itens de controlo, AL: Nível de avaliação)

O Segundo método consiste em calcular a soma total da avaliação dos valores dos detalhes do controlo de itens das respectivas categorias de controlo, a partir da seguinte fórmula:

$$M = \sum_{i=1}^{n} SAi \quad (3)$$

(M: soma total da avaliação dos valores dos detalhes de controlo de itens das respectivas categorias de controlo)

SAi: valores de avaliação dos detalhes de controlo de itens; n: Número de itens aplicados por cada categoria de controlo.

É calculado o resultado da soma da avaliação dos valores dos detalhes de controlo de itens, e os valores de cada categoria são expressos em percentagem.

$$LP = \frac{M}{N(\text{Soma dos itens})} * 100 \quad (4)$$

(Soma do número de itens aplicados à respectiva categoria)

A soma total dos valores percentuais (LP) por cada categoria de controlo dividida pelo valor da categoria de controlo é o valor percentual da avaliação do nivel de protecção da informação da agência avaliada.

$$AP = \frac{\sum_{i=1}^{12} LP}{N\ \text{itens}}$$

Os itens de controlo podem classificar-se como fortes ou vulneráveis no que respeita às ameaças de segurança, e isto permite aos gestores uma melhor detecção e correcção das suas vulnerabilidades.

O método apresentado por estes autores oferece-nos uma descrição pormenorizada das categorias de controlo, e como consequência, uma melhor compreensão dessas categorias,

dando assim um forte contributo para que haja uma melhor compreensão dos avaliadores dos níveis de protecção da informação das organizações, e desta forma para que haja uma maior eficácia na segurança da informação[40]

5 Partilha em segurança de informação

5.1 SOC: Centro de Operações de Segurança

SOC é o acrónimo de Centro de Operações de Segurança, que por sua vez é uma unidade – que funcionando de forma interna ou externa a uma organização – se dedica a observar sistemas e redes, contra-atacando eventuais ataques á Segurança da Informação, utilizando para isso: a analise estatística, a colecta e a gestão de Segurança da Informação em varias arquitecturas de sistema. O *staff* dedica-se á monitorização contínua de redes e facilidades de acesso aos sites, controlando também de forma directa ou indirecta os equipamentos de segurança dos sites. É pois possível ao SOC a detecção de potenciais ataques à segurança utilizando para isso os equipamentos de tecnologia de informação, que proporcionam uma contínua recolha de relatórios de acontecimentos, que são analisados e correlacionados em tempo real. Desta forma, é ainda tarefa do SOC prover resoluções para os ataques à segurança da Informação, protegendo e salvaguardando os sites. É ainda política de um Centro de Segurança de Operações eficiente, manter uma activa troca de informação sobre os eventos com outros Centros de Segurança de Operações.

Para além dos Centros de Operações de Segurança normais, existe o chamado ***National SOC***, ou Centro de Operações de Segurança Nacional, que é criado por um país, com o objectivo de proteger a tecnologia da informação mais importante que actua nos sites governamentais.

[40] *In* Yoo, Don-Young; Shin, Jong-Whoi; Lee, Gang-Shin, et al. (2007). "Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)." PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY: 6.

8.2 Partilha de Segurança de Informação

Uma vez que a adopção de alguns equipamentos de segurança da informação por parte do SOC se torna obsoleta ao lidar com certos tipos de ataque, logo que é detectado um ataque, o contra-ataque do SOC é feito através de um patch ao software do atacante, ou então, reconfigurando os seus próprios equipamentos face às características do atacante, colmatando depois as falhas ou vulnerabilidades do seu próprio sistema. Uma vez que os novos ataques têm tendência a causar muitos danos aos sites que 'visitam', é muito importante que haja uma partilha de informação entre os SOC's para controlar a expansão dos ataques e os danos causados por estes.

9 Mecanismos de partilha de segurança de informação

O objectivo de partilhar os ataques à segurança da informação é controlar os danos que estes provocam, devendo apenas ser partilhado o tempo em que ocorreu o ataque, a fonte do ataque, o nível do ataque e os destinatários. Contudo, os autores do artigo *A Trusted Security Information*, (Wu, Lu, Chen e Tsai, 2009) [41], defendem uma partilha de informação ainda mais reduzida baseada no formato SIDEx. Ainda segundo estes autores, existem mecanismos de autenticação utilizados entre os SOC's que podem ser utilizados para melhorar os níveis de segurança, assim como também podem ser utilizados os chamados percursos de protecção de dados os autores contribuem com varias sugestões para a construção de mecanismos de partilha de informação, a saber:

- A construção de um mecanismo de *trackback* que permita parar a expansão do ataque em tempo real, com base na identificação de *hosts* infectados e na distribuição de software de limpeza para eliminar ataques.
- Introduzindo uma plataforma de partilha de segurança da informação com base num reduzido *SIDEx* que tenha o potencial de 'esconder' automaticamente a informação sensitiva encaminhando a informação de acordo com o conjunto de critérios estabelecidos pelo emissor e pelo destinatário.
- Construir um sistema de gestão automática de redes que permita a reconfiguração automática dos equipamentos de rede de forma proporcional ao nível dos ataques detectados.

---

[41] *In* Tsai, Dwen-Ren; Chen, Wen-Chi; Lu, Yin-Chia; et al. (2009). A Trusted Security Information Sharing Mechanism. 2009 IEEE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY.

É muito difícil remover e detectar um novo tipo de ataque numa fase inicial, pelo que o Centro de Operações de Segurança deve estar habilitado para prevenir os sites circundantes e evitar que estes sejam afectados. Para que tal aconteça, é necessário que haja uma partilha de alguma informação entre os vários SOC's, partilha essa que apesar de necessária, se pretende que seja cada vez mais reduzida.

10 Prevenção da fuga de informação

10.1 Solução para Caso Prático – Ponto 2.5.1

Não se trata de uma solução mas apenas uma forma de contornar algumas vulnerabilidades. No que respeita à segurança da Informação no nível material, os responsáveis pela realização dos inquéritos BAD, sugerem algumas medidas que ao serem tidas em conta reduzem os riscos de destruição e violação da informação.

No que se refere às condições de segurança e aos edifícios, recomenda-se o apetrechamento de equipamentos de segurança apropriados para a redução do risco de perda de informação em caso de incidentes naturais; deverá ser instituído um plano de emergência;
Deve ser percebida a importância de elaborar planos de preservação e conservação de informação que respeitem os seguintes parâmetros: devem ter como ponto de referência projectos já elaborados e prever a definição de um orçamento específico, com a consequente atribuição de verbas; a definição de objectivos para concluir esses projectos; a selecção de um responsável por essa área.

No que diz respeito às condições ambientais, aconselha-se o fomento de acções de formação para consciencializar os profissionais sobre a importância de ter instalações com boas condições ambientais.

Quanto à gestão e controlo dos fundos e das colecções, deve ser incutida a necessidade de gerir e avaliar de forma eficaz não só o número de volumes existentes mas também a qualidade das colecções. Desta forma será possível determinar os eventuais 'desvios' de informação e fazer uma avaliação correcta da informação, de modo a ter uma percepção eficaz do que deve ser conservado e do que deve ser eliminado. É também sugerida a inclusão de linhas de financiamento que potenciem a criação de planos de preservação e conservação com o objectivo de impulsionar a criação de infra-estruturas regionais dividindo equitativamente os recursos humanos e equipamentos.

Por último, é fortemente recomendada a contratação de profissionais qualificados num número proporcional à eficácia dos serviços que as bibliotecas devem prestar aos seus

utilizadores, sendo por isso vivamente aconselhada a realização de cursos de reciclagem profissional e de formação contínua em PRECON[42].

Quanto à prevenção da informação em formato digital, seguem-se algumas sugestões: comecemos pela fuga de informação a nível informático, é cada vez mais importante investir em sistemas como programas de anti-virus ou de firewall, que bloqueiem as tentativas de violação e difusão de informação confidencial. No entanto muitas vezes as tecnologias informáticas não são suficientes para travar as fugas de informação, pelo que é muito importante apostar e investir na formação dos colaboradores, preparando-os para enfrentar esse tipo de desafios e evitar o desvio de informação da organização. Para além disso, é importante seleccionar bem os colaboradores que têm acesso a informação estritamente confidencial, uma vez que é arriscado deixar este tipo de informação ao alcance da pessoa errada. Para além disso, e talvez antes de qualquer uma dessas medidas devem ser respeitadas/seguidas as normas ISO 17799 e 27001[43].

11 Combate ao cibercrime

11.1 Centros de coordenação

Centros de Coordenação são centros que se dedicam à geração de respostas a incidentes à segurança da informação. Contribuindo de forma decisiva para o combate ao cibercrime.

11.1.1 CERT

Um dos mais importantes Centros de Coordenação é sem dúvida o **CERT/CC**, que embora tenha como missão inicial responder a incidentes, evoluiu para além disso, especializando-se na tarefa de identificar e calcular o tamanho das potenciais ameaças, planeando um contra-ataque a essas ameaças de forma coordenada com as equipas de resposta e com os fornecedores. O CERT está focalizado em várias áreas, desde a garantia do software até à segurança organizacional sem esquecer a segurança dos sistemas. Como é fácil depreender, estas áreas estão intimamente relacionadas entre si. Para garantir a segurança do software o CERT actua em vários níveis, como muitos programas de software facilmente evitáveis estão relacionados com o código de programação utilizado, é necessário garantir a segurança do código para que o software seja seguro, para isso, o CERT coloca alguns membros da sua equipa a trabalhar com profissionais e organizações de desenvolvimento de software com o objectivo de reduzir as vulnerabilidades provenientes de erros de código; para reduzir os riscos

---

[42] *In* Pinto, M. M. (2010). Apoio a Aulas 2**:** 46.

[43] *In* Leitão, H. F. (2008) O perigo vem de dentro. Fuga de Informação ou Desinformação **36**, 2

de segurança criados pelas vulnerabilidades do software, o CERT tenta abranger o número de vulnerabilidades tanto no software que está a ser desenvolvido como no software que já está implantado. Para corrigir eventuais vulnerabilidades, é utilizado um processo que compreende quatro passos: recolha, analise, coordenação e divulgação das vulnerabilidades, para garantir a segurança do software, o CERT desempenha ainda a função de excluir o código malicioso.

Para garantir a segurança do sistema, o CERT aposta num modelo de engenharia de segurança cibernética (ver anexo 3) e no desenvolvimento de soluções de engenharia e de abordagens de investigação com o objectivo de analisar a actividade que decorre na rede com o objectivo de caracterizar quantitativamente as ameaças e as actividades dos intrusos.

Na questão da segurança organizacional o CERT desenvolveu um guia para implementação da segurança nas organizações (ver anexo 4); verifica-se também uma preocupação em gerir a capacidade que o sistema tem para reagir face às alterações ou perturbações no seu meio envolvente. Para enfrentar isso, o CERT desenvolveu um modelo de gestão de resiliência baseado num processo de melhoria da segurança, de continuidade do negócio e em alguns aspectos da gestão de operações em Tecnologias da Informação. Esse processo é o conjunto das principais capacidades desempenhadas pela organização para assegurar que os seus 'bens' continuam a apoiar eficazmente os processos de negócio e os serviços. Como muitas vezes as maiores ameaças vêm de dentro e não de fora, esta área não é descartada pelo CERT, dedicando mesmo parte da sua atenção à pesquisa de ameaças internas. Para isso: procedem à avaliação do risco das ameaças internas, analisam um caso exemplo e descrevem as melhores práticas, fazem modelos e simulações, disponibilizam materiais de formação, tentam detectar e localizar as ameaças internas no ciclo de vida do desenvolvimento do software, publicam anualmente a revista electrónica "*e-crime watch survey*", e fazem pesquisa de espionagem[44].

11.2 Sancionamento do cibercrime: legislação aplicável

Para combater o *cibercrime*, foi aprovada pela Assembleia da República em 15 de Setembro do ano transacto uma proposta de lei[45]. Trata-se de uma lei que define as ordens penais materiais e processuais e a cooperação internacional relativamente ao *cibercrime*.

Algumas definições pertinentes na actual lei são: **Sistema informático:** todo o dispositivo ou rede de dispositivos envolvidos na execução de programas desenvolvendo o tratamento e a comunicação de dados informáticos, é ainda sinónimo de "Sistema informático" o conjunto de dados recuperados, tratados, armazenados ou transmitidos pelos referidos dispositivos; **Dados**

---

[44] *In* "CERT: Organizational Security." 2010, from http://www.cert.org/work/organizational_security.html.

[45] *In* Republica, A. d. (2009). Lei 109 de 2009, Assembleia da República: 7.

informáticos: toda a representação de dados, conceitos ou informações passíveis de serem processados num sistema informático; **Dados de tráfego:** dados informáticos associados a uma comunicação que se verifica através de um sistema informático criados por esse sistema como elementos de comunicação, indicadores do ponto de partida da comunicação, o trajecto, a hora, a data, o tamanho, a duração e o destino. **Fornecedor de serviço:** toda a entidade, publica ou privada, que possibilite aos seus utilizadores a comunicação através de um sistema informático, entende-se ainda por fornecedor de serviço qualquer entidade que proceda ao tratamento e armazenamento informáticos em nome próprio ou dos seus utilizadores; **Intercepção:** o acto de captar informações armazenadas num sistema informático utilizando dispositivos mecânicos, acústicos, electromagnéticos, etc; **Topografia:** uma serie de imagens associadas independentemente do modo de fixação e codificação que são uma representação tridimensional das camadas constituintes do produto semi-condutor correspondendo cada imagem a um desenho ou a parte dele e juntas (todas as imagens), formam a superfície do produto semi-condutor; **Produto semicondutor:** a forma final ou intermédia de qualquer produto informático composto por material semi-condutor e matérias condutoras ou semi-condutoras isolantes, assumindo uma representação tridimensional e desempenhando uma função electrónica (exclusiva ou não);

São susceptíveis de punição as seguintes actividades: a falsidade informática; os danos relativo a programas ou a outros dados informáticos; a destruição informática; o acesso ilegítimo; a intercepção ilegítima; a reprodução ilegítima de programa protegido…

A preservação de dados pode servir como constituição de prova. Quando necessário, as autoridades competentes ordenam a quem de direito que preserve os dados em causa. Essa preservação descrimina: a natureza dos dados; a origem e destino dos dados; e **o período de tempo atribuído à sua preservação** até um máximo de três meses. No entanto, pode ser ordenada a renovação da preservação de dados até um prazo máximo de um ano.

Quando necessário e se tal for ordenado pela autoridade judicial competente, a entidade que dispuser ou controlar os dados deve apresentá-los ou permitir o seu acesso. Se tal se verificar necessário, no decurso de um processo, a autoridade competente determina que se realize uma pesquisa no sistema em causa dirigindo essa pesquisa sempre que possível. Essa pesquisa tem de ser realizada no prazo máximo de 30 dias após a sua determinação. A pesquisa pode ser feita pela polícia criminal sem autorização prévia da autoridade judiciária quando se verificarem as seguintes condições:

1. For livremente consentida pela entidade que dispuser ou controlar os dados, sendo documentado esse consentimento;
2. Em caso de terrorismo, criminalidade violenta ou organizada, havendo suspeitas fundamentadas da prática de crime colocando em risco a vida ou a integridade das pessoas;

Confiscação de dados informáticos:

No decurso de uma investigação, quando forem encontrados dados ou documentos informáticos necessários á produção de prova para descobrir a verdade, a autoridade competente autoriza ou ordena a confiscação dos mesmos. Em caso de urgência ou de risco percebido na demora, podem ser feitas confiscações sem autorização prévia da autoridade judiciária. No caso de constar informação privada nos dados ou documentos apreendidos, estes são apresentados ao juiz, que determinará se devem ou não ser adicionados aos autos. As confiscações efectuadas pela polícia criminal têm de ser validadas em 72 horas.

Os dados informáticos podem ser confiscados das seguintes formas: apreensão do suporte de instalação do sistema ou do armazenamento dos dados informáticos, tal como dos dispositivos que a respectiva leitura requer; realização de uma cópia dos dados anexada posteriormente ao processo; apenas a preservação tecnológica da integridade dos dados e eliminação irreversível ou bloqueio de dados.

Detenção do correio electrónico e registo das comunicações de natureza similar:

Pode ser autorizada ou ordenada (pelo juiz) a apreensão de emails ou comunicações de natureza similar que possam ser importantes para o apuramento da verdade ou para a produção de prova.

Interceptar as comunicações:

Podem ser interceptadas as comunicações em crimes previstos na lei. Cometidos através de um sistema informático ou quando se verifica a necessidade de recolher prova em suporte electrónico;

Acções dissimuladas:

Em alguns casos é possível o recurso a acções dissimuladas, seguem-se alguns desses casos: crimes cometidos através de um sistema informático puníveis com pena de prisão superior a cinco anos, ou que atentem contra a liberdade e auto-determinação sexual – no caso de menores ou incapazes – burla qualificada, burla informática e nas telecomunicações, descriminação, fraudes económico-financeiras e crimes constantes do Código de Direitos de Autor e Direitos Conexos;

Cooperação internacional:

A cooperação internacional tem o objectivo de realizar investigações ou procedimentos associados a crimes associados a sistemas ou dados informáticos, tal como para a recolha de prova em suporte electrónico.

Cooperação internacional: ponto de contacto permanente

Existe uma estrutura assegurada pela polícia judiciária, que garante um ponto de contacto permanente, cuja assistência imediata inclui: aconselhamento técnico a outros pontos de contacto; preservação de dados em caso de urgência ou risco na demora; localização de suspeitos e fornecimento de informações de carácter jurídico; a transmissão imediata ao

Ministério Público de pedidos associados às medidas referidas nas duas alíneas anteriores, para serem rapidamente executados.

Cooperação internacional: preservação e revelação expeditas de dados informáticos:

Em caso de pedido de preservação expedita de dados informáticos, devem ser explicitados: a autoridade que pede a preservação; a infracção a ser investigada; os dados informáticos a preservar e a sua relação com o delito; informações disponíveis para identificar o responsável pela infracção, ou localizar o sistema informático; a necessidade que justifica a preservação; intenção de apresentar de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados.

Após isto a polícia judiciária ordena a preservação dos dados solicitados à entidade que os controlar ou deles dispuser. A ordem de preservação tem de especificar: a natureza dos dados; a sua origem e destino, se tal for possível; o período de preservação com um máximo de três meses, prazo esse que pode ser renovado pelo limite máximo de um ano; segue-se a preservação dos dados pelo período especificado, pela entidade respectiva; os dados apenas podem ser fornecidos:

1. À autoridade judiciária competente;
2. Á autoridade nacional que emitiu a ordem de preservação.

Os motivos que podem levar à recusa do fornecimento de dados: quando os dados respeitarem a lei portuguesa no que se refere à natureza política ou conexa; atentam contra os princípios da Constituição Portuguesa; não são oferecidas garantias de protecção dos dados pessoais; se prevê a recusa do pedido de auxilio por não se verificar a dupla incriminação;

Cooperação internacional: acesso a dados informáticos:

Para executar um pedido de uma autoridade estrangeira, a autoridade nacional competente pode pesquisar, apreender e divulgar dados informáticos armazenados em Portugal, tendo sido admissíveis a pesquisa e a apreensão num caso nacional similar. Suspeitando-se da vulnerabilidade dos dados informáticos relativamente à perda ou alteração, ou sendo prevista (em regulamento especifico) a rápida cooperação internacional, a autoridade nacional competente actua com a maior rapidez possível. O acesso transfronteiriço a dados informáticos armazenados e disponíveis publicamente ou com consentimento: as autoridades estrangeiras competentes podem, sem prévio consentimento das autoridades portuguesas:

1. Aceder a dados informáticos, armazenados em Portugal, que estejam publicamente disponíveis;
2. Receber ou ter acesso a dados informáticos cá armazenados, tendo o consentimento legal e voluntario da pessoa que pode legalmente divulgá-los;

Cooperação internacional: intercepção de comunicações:

Um juiz pode autorizar a intercepção de transmissões de dados informáticos num sistema localizado em Portugal, (desde que isso esteja legalmente previsto), para que se proceda

à execução de um pedido de uma autoridade estrangeira competente. A entidade competente para receber os pedidos de intercepção é a polícia judiciária que depois os transmite a quem de direito e esse despacho da autorização permite a transmissão imediata da comunicação para o Estado requerente;

12 Combate à engenharia social[46]

É necessário o desenvolvimento de políticas que comuniquem as preocupações relativamente aos ataques de engenharia social e dos hackers e treinar os colaboradores contra essas políticas para que se protejam a eles e às suas organizações. As organizações devem ser dotadas de um conjunto de políticas que apoiem a prevenção contra a engenharia social. Essa política, deve ser de fácil memorização e também devem ser facilmente implementadas quando se recebe uma chamada ou um *e-mail* suspeito. Devem ainda ser tomadas as seguintes medidas: ter em atenção a eventuais pedidos de informação não solicitados, sobre colaboradores, informação técnica, ou outros assuntos internos da organização; nunca fornecer *palavras-chave* ou *usernames* através de telefone ou *e-mail* a ninguém; não fornecer informações patronais, mas apenas á entidade patronal e mediante a apresentação da respectiva identificação; contactar as respectivas autoridades caso não haja certeza sob a legitimidade de um pedido; documentar e relate sempre situações suspeitas.

13 Porquê investir em investigação na segurança da informação?

As organizações aceitam, ou não põem em causa as necessidades de segurar os seus equipamentos, imóveis, viaturas, … uma vez que se mostram bens palpáveis, tangíveis. Porque não se manifesta, uma igual preocupação com a informação? Porque se encara tal investimento como uma despesa “desnecessária”, ou no mínimo “adiável”? Talvez a resposta possa residir no facto da informação não ser um bem visível e palpável pela organização. Parece importante incidir neste aspecto.

Como prevenir então eventuais problemas de segurança da informação? O sucesso de um programa de segurança de informação, reside em analisar os pontos fracos da organização e melhorá-los, evitando que essas fraquezas sejam utilizadas para violação da informação.

Os ataques maliciosos a infra-estruturas das empresas tornaram-se uma séria ameaça com o crescimento da internet. Cada vez mais as organizações têm que implementar uma espécie de “salvaguarda” que assegure a confiabilidade, integridade, e a disponibilidade da informação. Falhas a este nível, tornam as organizações vulneráveis e conduzem a prejuízos

[46] *In* Thompson, Samuel T. C. "Helping the Hacker." *Information Tecnology & Libraries* 25, no. 4 (2006): 5.

financeiros e a perdas de clientes e bens. Segundo vários estudos, foram já apresentados vários modelos com o propósito de justificar a importância em investimentos em segurança de informação, ao nível organizacional. Esses modelos são limitados pela dificuldade ou falta de fiabilidade na prevenção de potenciais perdas relacionadas com a existência de lacunas na segurança e a previsão dessas próprias lacunas. Uma simples falha na segurança da informação envolvendo acesso não autorizado por parte de utilizadores – por exemplo, o acesso à informação constante no cartão de crédito – pode ter consequências catastróficas para uma organização.

No estudo *Quantifying the Benefits of Investing in Information Security*[47], elaborado por *Khansa e Liginlal*, é proposto um modelo baseado no valor da flexibilidade da "troca" entre Tecnologias de Informação Compatíveis. Mencionam outros autores como *Ettredge* e *Richardson*, que expõem os efeitos nefastos que as lacunas de segurança provocam no mercado de valor das organizações.

No modelo apresentado, é medido o investimento global em segurança da informação de acordo com as receitas apresentadas pelas firmas que, dedicando-se á segurança da informação, controlam a partilha entre os vários segmentos de mercado de segurança da informação. Para tal é proposto o seguinte: o investimento em segurança da informação é eficaz na redução de muitos "ataques maliciosos" que são conhecidos por afectarem negativamente o valor das acções das organizações; e um maior pedido de produtos e serviços de segurança da informação indica uma perspectiva positiva para a mesma e é sinónimo de um aumento do valor das acções que lidam com a segurança da informação.

É proposto que a soma das receitas obtidas pelas empresas de segurança da informação, que controlam o respectivo mercado constituam, um bem mensurável para o cálculo global em segurança da informação.

Neste estudo foram recolhidas 6.400 situações de "ataques maliciosos" apenas no website da Symantec[48]. Os níveis de gravidade dos ataques foram classificados por assunto com base em três atributos, nomeadamente, poder de destruição, distribuição e violência – refere-se à expansão do ataque/ ameaça no computador dos utilizadores. Poder de destruição está relacionado com os danos ou com os potenciais danos. E a distribuição está relacionada com a velocidade de expansão do ataque.

Para avaliar a necessidade de investimento em segurança da informação, os autores do estudo recolheram todas as receitas trimestrais e dados de mercado de valores, tendo como fonte o banco de dados *CRSPg*. Para a sua análise foram utilizadas as seguintes variáveis: receitas; retorno do mercado; preço de stock e a gravidade dos ataques.

---

[47] *In* Khansa, L.; Liginlal, D. (2009). "Quantifying the Benefits of Investing in Information Security." Communications of the Acm **52**(11): 6.

[48] Empresa líder no fornecimento de software anti-vírus.

Assim, pode dizer-se que se uma organização não der a devida importância à segurança da informação vai ser mais desacreditada no mercado, uma vez que os clientes não vão ter grande confiança nessa organização.

Pelo contrário, se a organização se preocupar em colmatar as lacunas de segurança da informação (não há um sistema de segurança da informação perfeito), vai ganhar valor aos olhos do cliente e vai aumentar o seu valor de mercado[49].

Conclusão

A Segurança da Informação está relacionada com protecção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações electrónicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de protecção de informação. O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança informação, mas também a dos sistemas em si. Embora essa protecção, não se deva encarar apenas no sentido digital e informático, mas ao nível, chamado tradicional. A segurança da Informação, pode e dever ser medida a dois níveis: a um nível físico, que compreende, como o próprio nome indica, as ameaças físicas, como: incêndios, desabamentos, relâmpagos, inundações, acesso indevido de pessoas, forma inadequada de manuseamento e tratamento do material, etc; e a um nível lógico – atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, *backups* desactualizados, violação de palavras-chave, etc.

A informação, definida em Ciência da Informação como - *conjunto estruturado de representações mentais e emocionais codificadas (signos e símbolos) e modeladas com/pela interacção social, passíveis de serem registadas num qualquer suporte material (papel, filme, banda magnética, disco compacto, etc.) e, portanto, comunicadas de forma assíncrona e multi-direccionada, é cada vez mais um bem considerado de grande valor.*

Vivemos numa sociedade que se baseia em informação e que exibe uma crescente propensão para obter e armazenar informação e o uso efectivo da informação permite que uma organização aumente a eficiência de Operações já o afirma *Katzam*, 1977.

---

[49] *In* Khansa, L.; Liginlal, D. (2009). "Quantifying the Benefits of Investing in Information Security." Communications of the Acm **52**(11): 6.

A informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade (*Rezende e Abreu, 2000).* E percebeu-se aqui *que as* as empresas já perceberam, ou tendem cada vez mais a perceber que o domínio da tecnologia como aliado para o controlo da informação é vital e que o controlo da informação é um factor de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial já o defendiam *Synnat,* 1987; *Feliciano Neto, Furlan e Higo,* 1988.

Dispor da informação certa, na hora certa, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos dados e sistemas, a informação ganhou mobilidade, inteligência e real capacidade de gestão, daí a importância em proteger e guardar adequadamente esse bem chamado informação.

Actualmente o conceito de Segurança da Informação está padronizado pela as normas ISO 17799, ISO 27000 e ISO que foram reservadas para tratar de padrões de Segurança da Informação. Que como se percebeu, e embora as normas nem sempre sejam passíveis de ser utilizadas pelas instituições, e a sua eficácia não corresponda a 100%, são instrumentos que (quando adoptados), permitem às instituições ultrapassar muitas vulnerabilidades relacionadas com a segurança da informação. Desta forma, tornam-se mais eficazes no combate à informação, e inspiram mais confiança aos utilizadores, o que permite o sucesso. A Segurança da Informação refere-se à protecção existente sobre a informação de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais. Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afectada por factores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objectivo de furtar, destruir ou modificar tal informação.

Portanto os atributos básicos, segundo os padrões internacionais ISO/17799 são: a confidencialidade - propriedade que limita o acesso a informação tão-somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação; a integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controlo de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição); e a disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, pelos utilizadores autorizados pelo proprietário da informação.

Listaram-se aqui alguns mecanismos para atestar a segurança da informação e o suporte para as recomendações de segurança pode ser encontrado em: *controlos físicos*: são barreiras que limitam o contacto ou acesso directo à informação ou a infra-estrutura (que garante a

existência da informação) que a suporta. E existem mecanismos de segurança que apoiam os controlos físicos. E *controlos lógicos*: são barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente electrónico, e que, de outro modo, ficaria exposta a alteração não autorizada por alguém mal intencionado.

Existem uma serie de regras que, sendo seguidas – embora não garantam uma protecção total da informação – ajudam a prevenir e contornar algumas vulnerabilidades das instituições no que se refere à protecção da informação. Perspectivou-se aqui como se procede ou deve proteger a informação contra roubos, catástrofes naturais, …

Os mecanismos de segurança que apoiam os controlos lógicos: são por exemplo: *mecanismos de criptografia*: utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptográficos, produzir uma sequência de dados criptográficos; a *assinatura digital*, que é um conjunto de dados criptográficos, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade; *mecanismos de garantia da integridade da informação*, usando funções de "Hashing", por exemplo; m*ecanismos de controlo de acesso*, com o uso de palavras-chave, sistemas biométricos, *firewalls*, etc; m*ecanismos de certificação* que atestam a validade de um documento, e ainda um outro vasto conjunto de mecanismos.

Com a integração da Internet no quadro comunicacional de grande parte das organizações, assistiu-se à invasão de uma multiplicidade de técnicas, métodos ou mecanismos de software malicioso que surgiram com o intuito de violar a informação, e mais alarmante ainda é o facto da grande maioria dos *ciber-ataques* a seguir descritos terem origem no interior das organizações, e os mecanismos mencionados anteriormente, surgiram com o intuito de proteger a informação, a todos os níveis, contra esses ataques, estando ou não ligadas ao quadro computacional e informático.

Foi aqui apresentado e percebido a importância da existência de um método para que se componham procedimentos destinados a medir o nível de segurança da organização; a existência de Centros de Operações de Segurança, como SOC, que se dedica a observar sistemas e redes, contra-atacando eventuais ataques á Segurança da Informação, utilizando para isso: a analise estatística, a colecta e a gestão de Segurança da Informação em varias arquitecturas de sistema., e do **CERT/CC**, um dos mais importantes Centros de Coordenação especializando na tarefa de identificar e calcular o tamanho das potenciais ameaças, planeando um contra-ataque a essas ameaças de forma coordenada com as equipas de resposta e com os fornecedores.

Compreende-se por fim que numa organização, tudo está ligado à informação, ela é extremamente importante dentro de uma empresa, dessa forma a sua segurança é de extrema importância. Porém, a maioria das empresas, não vêem, ou não viam essa necessidade, por se considerar que os resultados dela, não são muito visíveis como um sector que atinge a sua meta antes do tempo, possuindo resultados mais visíveis e concretos.

A segurança da informação funciona a longo prazo, fazendo uma harmonização de seus processos, tarefas, pretendendo dessa forma amenizar os erros e não repassar informações desnecessárias ou sem importância. Uma grande empresa, com filiais, que possui um sistema de informação integrado, contendo todas as informações de todas as filiais, precisa ter um sistema integrado e automatizado de backup periódico, firewall, sistemas de segurança física, lógica e pessoal… se ela perder toda a informação, provavelmente, a empresa, ou individuo, perderá um valor incalculável.

Por exemplo, se a organização se preocupar em colmatar as lacunas de segurança da informação (não há um sistema de segurança da informação perfeito), vai ganhar valor aos olhos do cliente e vai aumentar o seu valor de mercado.

14 Referências Bibliográficas

- "CERT: Organizational Security." 2010, from http://www.cert.org/work/organizational_security.html.
- "Colégio Web." Retrieved 2010, from http://www.colegioweb.com.br/curiosidades/biometria.html.
- "Kimaldi: Àrea de Conhecimento Assinatura Digital." From http://www.sankhya.com.br/glossario_a.php.
- Multicert. "Certificados digitais." 2010, from https://www.multicert.com/certificadosdigitais.
- "Resultado! Concursos Notícias e Editais de Concursos Públicos 2010 – Provas, Gabaritos, Apostilas, Resultados e mais." 2010.
- "SANKHYA: Gestão de Negócios." from http://www.sankhya.com.br/glossario_a.php.
- "WebHouse.Net: Glossário de Termos da Internet." Retrieved 2010.
- (2004). Incêndio destroi património da humanidade. DW-WORLD. DE, B2B.
- (2009). "Guia Prático para a Internet e as Novas Tecnologias." Internet e Novas Tecnologias: 16.
- Departamento de Ciência da Informação, C. d. C. J. e. E., UFES - Universidade Federal do Espírito Santo; and F.-F. d. L d. U. d. P. Secção Autónoma de Jornalismo e Ciências

da Comunicação Ciência da Informação. Dicionário Electrónico de Ciência da Informação.

- Departamento de Ciência da Informação, C. d. C. J. e. E., UFES - Universidade Federal do Espírito Santo; and F.-F. d. L. d. U. d. P. Secção Autónoma de Jornalismo e Ciências da Comunicação. Dicionário Electrónico de Ciência da Informação.

- Depósitos, C. G. d. "Glossário de Segurança." 2010, from http://www.cgd.pt/Seguranca/Glossario/Pages/Seguranca-Glossario.aspx.

- ISO (2005). ISO 17799. Suíça, ISO. **17799.**

- ISO (2005). ISO 27001. Suíça, ISO. **27001**.

- Cicco, F.(2006)ISO/IEC 27001 na opinião de um especialista.3

- Laureano, M. A. P. (2005) Gestão de Segurança da Informação. 132

- Yoo, Don-Young; Shin, Jong-Whoi; Lee, Gang-Shin, et al. (2007). "Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)." PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY: 6.

- Leitão, H. F. (2008) O perigo vem de dentro. Fuga de Informação ou Desinformação **36**, 2

- Khansa, L.; Liginlal, D.(2009). "Quantifying the Benefits of Investing in Information Security." Communications of the Acm **52**(11): 6.

- Lynch, D. M. (2006). "Security Against Insider Attacks." Information Security Journal **15**(5): 9.

- Main, A. (2004). "Application Security: Building in Security during the Development Stage." Information Security Journal **13**(2): 7.

- Knapp, K; Marshall, T.; JR. Rainer, R. K., et al.(2006). "The Top Information Security Issues Facing Organizations: What Can Government Do to Help?" Information Security Journal **15**(4): 8.

- Reinhold, C.; Frolick, M.; Okunoye, A.(2009). "Managing Your Security Future." Information Security Journal **18**(3): 8.

- Ott, J. L. (2000). "Information Security in the New Millenium." Information Security Journal **9**(1): 3.

- Pinto, M. M. (2010). Apoio a Aulas 2**:** 46.

- Pinto, M. M. (2010). Apoio a Aulas 3**:** 96.

- Reed, B. (2007). "Implementing Information Lifecycle Security." Information Security Journal **16**(3): 5.

- Republica, A. d. (2009). Lei 109 de 2009, Assembleia da República**:** 7.

- Santos, H. Gestão da Segurança da Informação. Porto, Universidade do Porto**:** 10.

- Thompson, Samuel T. C. "Helping the Hacker." Information Tecnology & Libraries 25, no. 4 (2006): 5.

- Tsai, Dwen-Ren; Chen, Wen-Chi; Lu, Yin-Chia; et al. (2009). A Trusted Security Information Sharing Mechanism. 2009 IEEE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY.

Anexos

Norma ISO 17799

VER PASTA

Norma ISO 27001

VER PASTA

Lei do Cibercrime

VER PASTA